HP Modular Cooling System Web Interface User Guide

Part Number 403358-002
February 2007 (Second Edition)

Contents

Overview

In this section

Introduction

The HP Modular Cooling System has a management module with a web interface that analyzes, queries, and manages various measurements, and warning and alarm messages from the MCS unit.

The management module analyzes measurements provided by each cooling module, generates any necessary warning or alarm messages, and sends them to the web interface. When a new warning or alarm occurs, the warning and alarm messages (on page 10) appear on the operator display, as well as on the web interface Alarms menu, Alarm History menu, and an SNMP trap is sent to up to four trap receivers ("Trap Receivers tab" on page 35). An alarm relay is also activated (if enabled), and an alarm is signaled acoustically by the MCS unit internal beeper (if enabled in the appropriate web interface menu). For more information on connecting an alarm device to the management module alarm relay, see the *HP Modular Cooling System User Guide.*

The web interface (on page 6) displays various measurements and warning and alarm messages (on page 10) from the management module. Also, various system values can be set through the web interface and sent to the management module. The MCS unit can be monitored with HP SIM. For more information, see "HP Systems Insight Manager integration."

Web interface requirements

The following table lists the minimum requirements necessary to operate the web interface.

Software	**Browser**
Web browser on a client	• Microsoft® Internet Explorer 6.0 with Service Pack 1 (32-bit only) • Red Hat Linux operating system (32-bit only) • Mozilla 1.4 • SUSE LINUX operating system (32-bit only) • Mozilla 1.6
Monitor resolution	Minimum supported resolution of 1024 x 768, 16-bit high color (maximize browser window for optimal display)
Desktop resolution	SLES 9 Mozilla 1.6 1 Right-click the mouse, and select **Configure Desktop.** 2 Select **1152 x 864.** 3 Select **75 Hz.**

Web interface

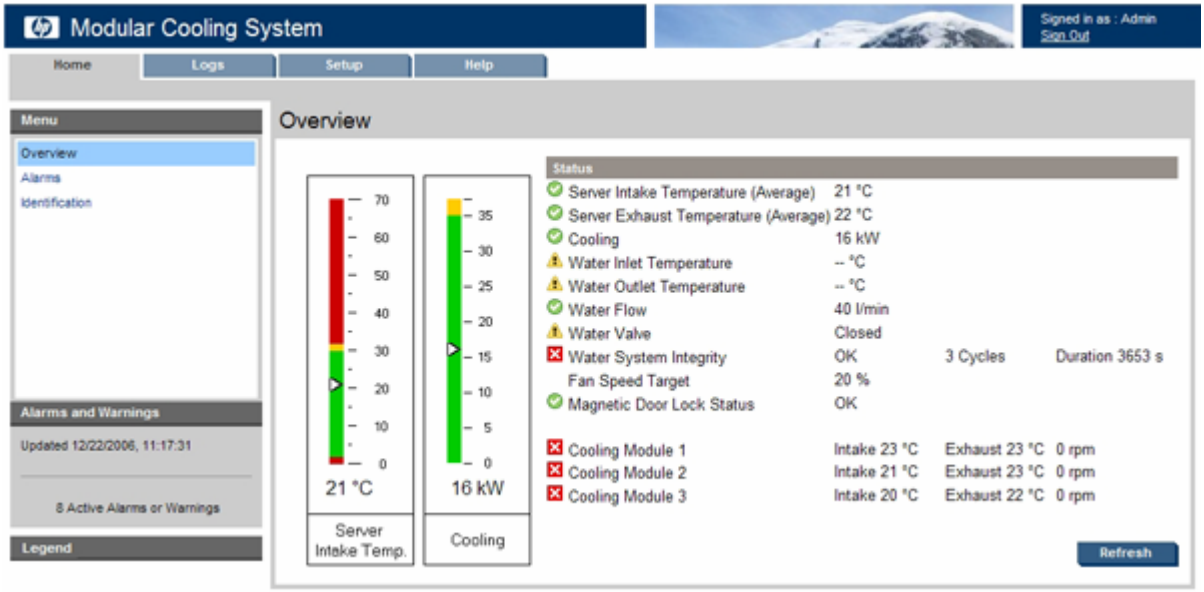
In this section

Using the web interface

The web interface is divided into three frames:

- **Top frame**—Contains a Sign Out hyperlink and the Home, Logs, Setup, and Help tabs.
  - Click **Sign Out** to log out of the web interface.
  - Click **Home** to see the menu options for viewing general status information. For more information, see "Home tab (on page 8)."
  - Click **Logs** to see the menu options for displaying data logs. For more information, see "Logs tab (on page 21)."
  - Click **Setup** to see the menu options for configuring the management module and setting up and modifying user accounts. For more information, see "Setup tab (on page 23)."
  - Click **Help** to access the web interface information and help section. For more information, see "Help tab (on page 39)."
- **Left navigation frame**—Contains a list of menu options, a list of alarms and warnings, and a legend.
  - The options menu is dynamic, and the options listed change depending on the tab selected and your access rights.
  - The list of alarms and warnings displays the individual alarm status for each managed MCS unit. The graphical indicator displays the number of active alarms and displays the icon for the most severe alarm. The date and time of the last update is also indicated.
  - The legend displays the meaning of symbols used in the interface. Expand and collapse the legend by clicking the arrow in the upper right corner.

- **Main frame**—Contains the various web interface screens based on the menu option selected in the left navigation frame.



Active Alarms and Legend display panel

Each tab in the web interface contains an Active Alarms and Legend display panel.

When the MCS unit experiences a critical, warning, normal, unknown, or informational event, the icon corresponding to the event appears in the Active Alarms display panel. The alarm descriptions appear in the Alarms menu, as well as in the Alarm History menu.

In the Legend display panel, the descriptions for following five icons display:

Icon	Reference	Description
	Critical	Appears when a parameter is not operating at a normal condition and must be investigated immediately
	Warning	Appears when a parameter is not operating at a normal condition and must be investigated
	Normal	Appears when all parameters are operating at a normal condition
	Unknown	Appears when a parameter is operating at an unknown condition
	Information	Displays information about a parameter

Accessing the management module through the web interface

1. Launch a supported browser. The browser window appears.
2. In the Address field (Microsoft® Internet Explorer) or the Location field (Mozilla), enter one of the following:

   `http://`*hostname[:port number]*

   -or-

   `https://`*hostname[:port number]* (if SSL is enabled)

where *hostname* is the IP address of the management module and *port number* is the port number if using a port other than the default 80 for http and 443 for https. The login screen appears.

3. Log in through the web browser.

Logging in through the web interface

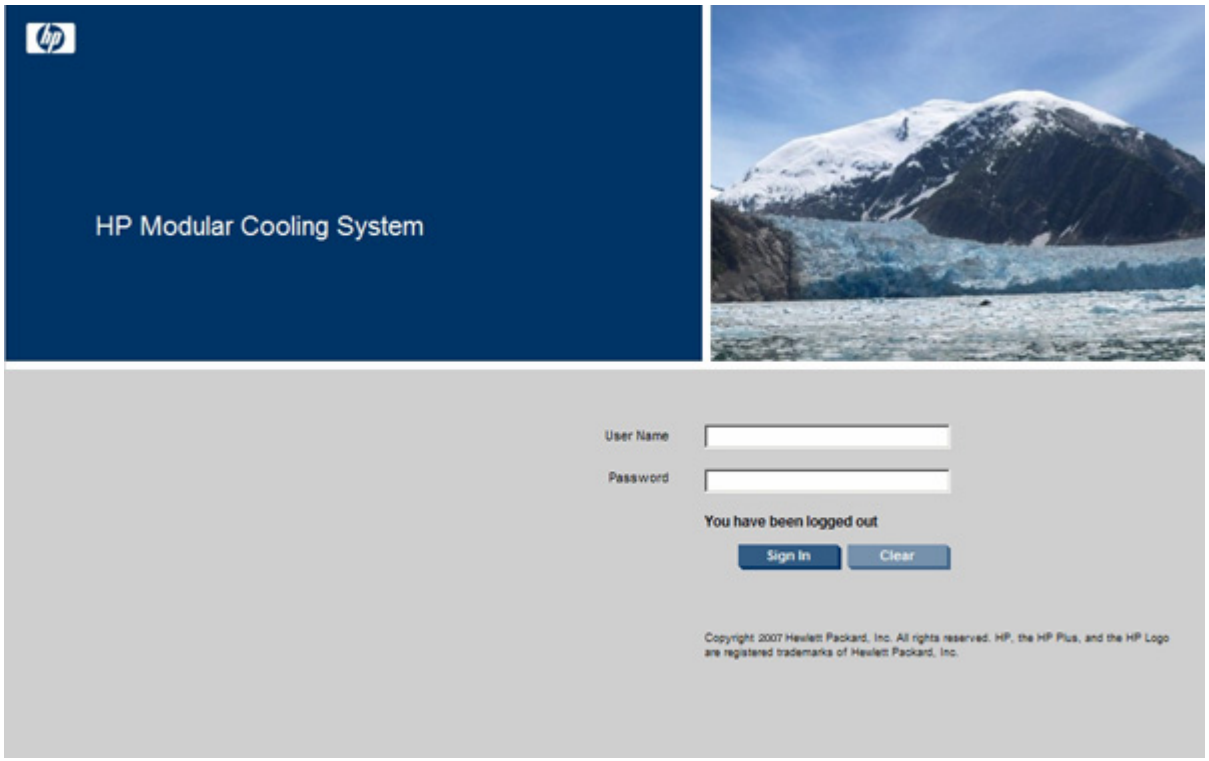
1. Enter the user name in the User Name field. The default user name is `Admin`.
2. Enter the password in the Password field. The default password is `Admin`.

NOTE: Passwords are case-sensitive.

3. Click **Sign In.** The HP Modular Cooling System web interface appears.

To clear the credentials and enter another user name and password, click **Clear**.

For instructions on changing the password, see "Accounts menu (on page 37)."



Only one Admin session and one User session are supported at a time. Sessions can be terminated if a second session is initiated (after successful login) or if a console session timeout occurs. In both situations, the existing session is terminated and the login screen appears. Admin session logins, logouts, and terminations are recorded in the Event Log menu. The console session timeout length can be enabled, disabled, or modified in the Remote Access tab. The default is 30 minutes.

Home tab

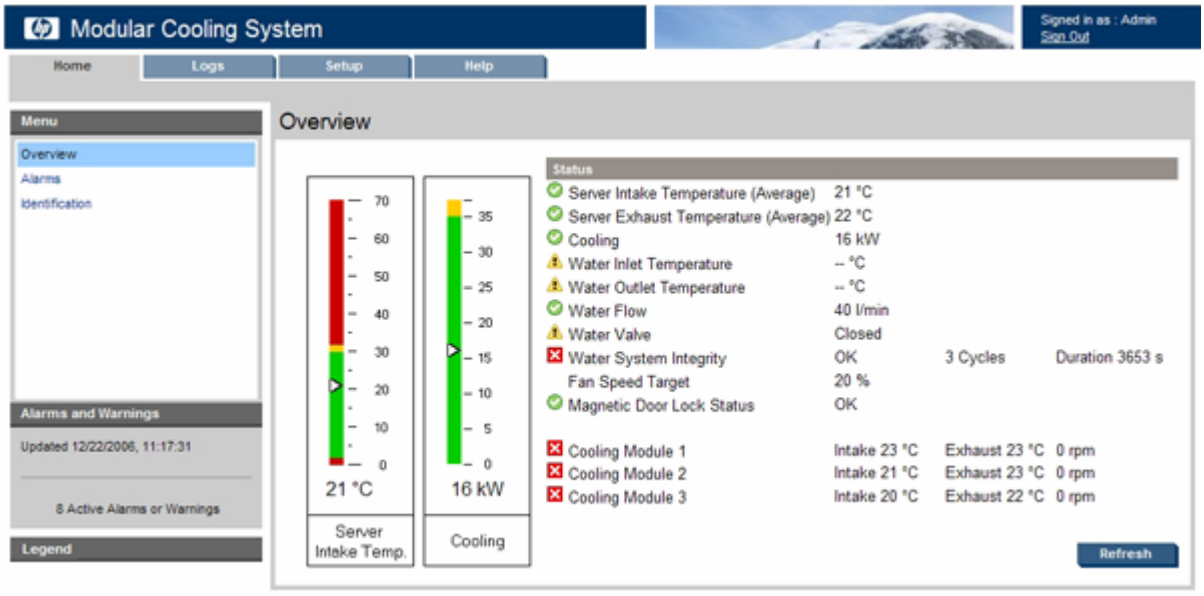
Menu options listed under the Home tab include:

- Overview menu
- Alarms menu

- Identification menu

Overview menu

Click **Overview** in the left navigation frame to display the Overview screen. This screen displays graphic meters for temperature and cooling system parameters.



Parameter	Function
Server Intake Temperature (Average)	Displays the average server intake temperature
Server Exhaust Temperature (Average)	Displays the average server exhaust temperature
Cooling	Displays the total heat removed by the water
Water Inlet Temperature	Displays the temperature of the water coming into the MCS unit to be used to cool the servers
Water Outlet Temperature	Displays the temperature of the water after removing the server heat
Water Flow	Displays the water flow rate in liters or gallons per minute
Water Valve	Displays the water valve state
Water System Integrity	Displays the Leak Detected Alarm, the Condensation Pump Warning, and condensation pump activity • Cycles displays the number of times the pump runs. • Duration displays the total amount of time the pump has run since it was last activated.
Fan Speed Target	Displays the percentage of the maximum fan speed

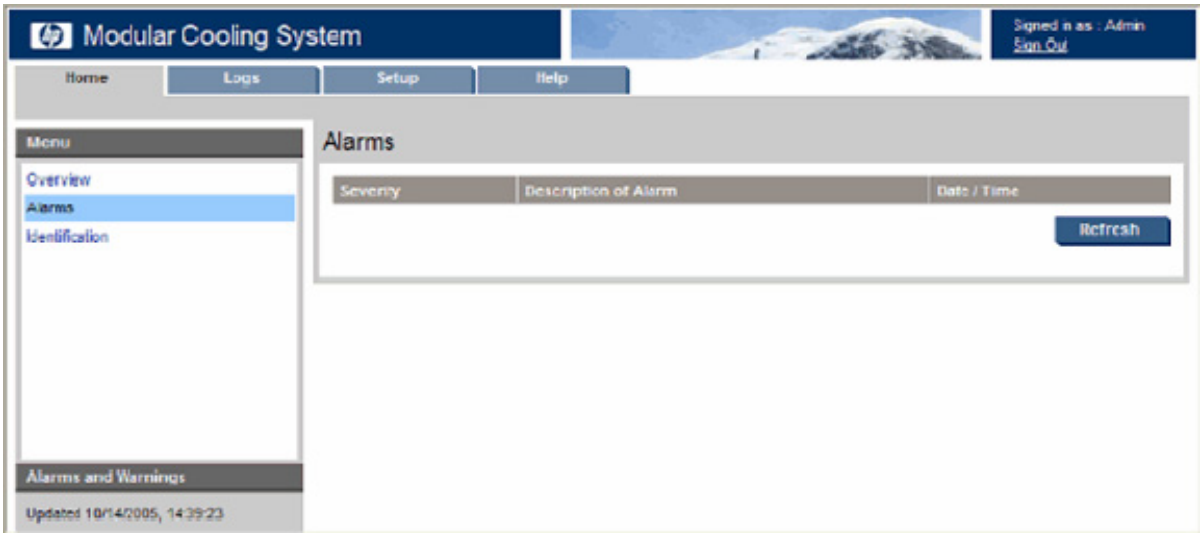
Parameter	Function
Magnetic Door Lock Status	Displays the door lock status • **OK** means the door lock is functioning properly and the door magnet is engaged. • **Doors Released** means there is an emergency door condition and the door magnet has released the doors.
Cooling Module 1, 2, and 3	Displays the Server Intake and Server Exhaust temperature and the RPM of each cooling unit

Alarms menu

Click **Alarms** in the left navigation frame to display the Alarms screen. The active alarms are listed by the date and time at which the alarm most recently occurred. The active alarm is removed from the Alarms screen when cleared but is recorded in the Alarm Log.

The following information appears for each alarm:

- **Severity**—An icon indicating the severity or status of the alarm (Critical, Warning, Normal, Unknown, or Information)
- **Description of Alarm**—The name of the alarm (For more information on the alarm description, see "Warning and alarm messages (on page 10).")
- **Date/Time**—The date and time at which the alarm occurred



On the Alarms screen, click **Refresh** to update the screen with current information.

Warning and alarm messages

The following tables describe the possible warning and alarm messages that are sent to the management module from the MCS unit and appear on the operator display, and on the web interface Alarms menu and Alarm History menu.

Fan unit failed

Indicators	Meaning
Actual operator display alarm message	Top, Mid, or Bot Fan Mod. Failed
Actual web interface alarm message	Top, Mid, or Bottom Fan Module Failed
Condition	Top, middle, or bottom fan module tach is less than its minimum rpm
Module	Top, middle, or bottom fan module
SNMP notification	Warning
Type of message	Warning

Solution:

1. Remove the fan unit.
2. Reinstall the same fan unit.

If the warning message does not clear after the module is reseated, replace the fan unit with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

Fan unit not installed

Indicators	Meaning
Actual operator display alarm message	Top, Mid, or Bot Fan Not installed
Actual web interface alarm message	Top, Middle, or Bottom Fan Not installed
Condition	Failed connection to the fan unit sensors over the I²C bus (possible open circuit)
Modules	Top, middle, or bottom fan module
SNMP notification	Warning
Type of message	Warning

Solution:

1. Remove the fan unit.
2. Reinstall the same fan unit.

If the warning message does not clear after the module is reseated, replace the fan unit with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

HEX (heat exchanger unit) temperature in failed (Server Intake Temperature failed)

Indicators	Meaning
Actual operator display alarm message	HEX1, HEX2, or HEX3 Temp. In Failed
Actual web interface alarm message	Top Heat Exchanger Intake Air Temperature Sensor to Server Failed
Condition	Temperature reading is beyond limit (possible open circuit)

Indicators	Meaning
Sensors	HEX1, HEX2, or HEX3 sensors (this is the water to air heat exchanger unit temperature of the intake to the servers)
SNMP notification	Warning
Type of message	Warning

Solution:

1. Remove the fan unit.
2. Remove the HEX unit.
3. Reinstall the same HEX unit.
4. Reinstall the same fan unit.

If the warning message does not clear after the module is reseated, replace the HEX unit with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

HEX temperature out failed (Server Exhaust Temperature failed)

Indicators	Meaning
Actual operator display alarm message	FAN1, FAN2, or FAN3 Temp. Out Failed
Actual web interface alarm message	Top Fan Exhaust Air Temperature Sensor from Server Failed
Condition	Temperature reading is beyond limit (possible open circuit)
Sensors	FAN1, FAN2, or FAN3 sensors (this is the fan unit temperature of the exhaust from the servers)
SNMP notification	Warning
Type of message	Warning

Solution:

1. Remove the fan unit.
2. Reinstall the same fan unit.

If the warning message does not clear after the module is reseated, replace the fan unit with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

Air temperature sensor failed

Indicators	Meaning
Actual operator display alarm message	Air Temp. Sens Failed
Actual web interface alarm message	Air Temperature Sensor Failed
Condition	Single air temperature sensor is significantly different from the others
Sensors	Air temperature sensors
SNMP notification	Warning
Type of message	Warning

Solution:

1. View the Overview menu to distinguish which temperature sensor is different from the other temperature sensors.
2. After discovering which temperature sensor is not working properly, remove that module and reinstall it. If the difference is in the Server Exhaust Temperature, replace the appropriate fan unit. If the difference is in the Server Intake Temperature, replace the appropriate HEX unit.

If the warning message does not clear after the module is reseated, replace the HEX unit with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

Low water flow

Indicators	Meaning
Actual operator display alarm message	Water flow Low
Actual web interface alarm message	Water flow Low
Condition	No or low water flow
Modules	Water group
SNMP notification	Warning
Type of message	Warning

Solution:

Verify the water supply.

Water temperature input is out of range

Indicators	Meaning
Actual operator display alarm message	Water Temp. In Failed
Actual web interface alarm message	Water Unit Temperature Input Out of Range
Condition	Water temperature sensor is not working properly (possible open circuit)
Sensors	Water group sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify the water supply.
2. Verify whether the water temperature is below or above the water temperature expected range.
3. Contact your building supervisor.
4. Contact HP, or see the HP website (http://www.hp.com).

Water temperature output is out of range

Indicators	Meaning
Actual operator display alarm message	Water Temp. Out Failed
Actual web interface alarm message	Water Unit Temperature Output Out of Range
Condition	Water temperature sensor is not working properly (possible open circuit)
Sensors	Water group sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify the water supply.
2. Verify whether the water temperature is below or above the water temperature expected range.
3. Contact your building supervisor.
4. Contact HP, or see the HP website (http://www.hp.com).

Water flow sensor is not working properly

Indicators	Meaning
Actual operator display alarm message	Water flow Sensor ?
Actual web interface alarm message	Water flow Sensor Value Out of Range
Condition	Water flow sensor is not working properly
Sensor	Water group
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify the water supply.
2. Contact HP, or see the HP website (http://www.hp.com).

Water flow valve is closed

Indicators	Meaning
Actual operator display alarm message	Water Valve ?
Actual web interface alarm message	Water Valve Failed
Condition	Water flow valve is closed and water flow is detected
Modules	Water group
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify the water valve is closed.
2. Contact HP, or see the HP website (http://www.hp.com).

Leak detector sensor is not working properly

Indicators	Meaning
Actual operator display alarm message	Leak detector?
Actual web interface alarm message	Leak detector Failed
Condition	Leak detector sensor is not working properly
Sensors	Leak detector sensor
SNMP notification	Warning
Type of message	Warning

Solution:

Contact HP, or see the HP website (http://www.hp.com).

Uneven heat load

Indicators	Meaning
Actual operator display alarm message	Heat Load?
Actual web interface alarm message	Heat Load Warning
Condition	Measured air temperature values dramatically different from top to bottom
Sensors	Air temperature sensors
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify that nothing is blocking the heat path.
2. Verify that the server is loading.
3. Adjust the Temperature Difference for Heat Load Warning in the Advanced tab (on page 29).

Heat overload condition (High Temperature Threshold field)

Indicators	Meaning
Actual operator display alarm message	Temperature Warning
Actual web interface alarm message	Temperature Warning
Condition	Heat overload condition
Modules or sensors	Average server air temperature is above the temperature assigned in the web interface Intake Temp tab High Temperature Threshold field
SNMP notification	Critical
Type of message	Alarm

Solution:

1. Verify the water inlet temperature.
2. Verify that the flow matches the specifications required for heat load.
3. Adjust the temperature assigned in the web interface Intake Temp tab High Temperature Threshold field.

Leakage detected

Indicators	Meaning
Actual operator display alarm message	Leakage Detected
Actual web interface alarm message	Leakage Detected
Condition	Leak is detected
Modules or sensors	Leakage detector actuated
SNMP notification	Critical
Type of message	Alarm

Solution:

1. Open the rack doors.
2. Power down the rack-mounted components.
3. Turn off the water to the MCS unit.
4. Locate the leak and correct it.

Communication failure

Indicators	Meaning
Actual operator display alarm message	Comm. Failure I²C
Actual web interface alarm message	Comm. Failure I²C
Condition	Management module cannot communicate with the MCS unit sensors
Modules or sensors	Any module or sensor
SNMP notification	Critical
Type of message	Alarm

Solution:

Power cycle the management module. If the alarm message continues to display, replace the management module with a CSR part. For more information on CSR parts, see "Replaceable parts and maintenance and service information (on page 55)."

Temperature below threshold (Low Temperature Threshold field)

Indicators	Meaning
Actual operator display alarm message	Temperature Too low

Indicators	Meaning
Actual web interface alarm message	Temperature too low
Condition	Average server air temperature is lower than the temperature assigned in the web interface Intake Temp tab (on page 24) Low Temperature Threshold field
Sensors	Air temperature sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify water flow matches specifications required for heat load.
2. Verify whether the water temperature is below the expected range.
3. Adjust the temperature assigned in the web interface Intake Temp tab (on page 24) Low Temperature Threshold field.
4. Contact your building supervisor.

Temperature above threshold (Warning Temperature Threshold field)

Indicators	Meaning
Actual operator display alarm message	Temperature Too high
Actual web interface alarm message	Temperature too high
Condition	Average server air temperature is above the temperature assigned in the web interface Intake Temp tab (on page 24) Warning Temperature Threshold field
Modules or sensors	Air temperature sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Verify water flow matches specifications required for heat load.
2. Verify whether the water temperature is above the expected range.
3. Adjust the temperature assigned in the web interface Intake Temp tab (on page 24) Warning Temperature Threshold field.
4. Contact your building supervisor.

Emergency Door Opening due to Water Flow Loss (0 l/min; 36/34/35°C) (0 gal/min; 97/93/95°F)

Indicators	Meaning
Actual operator display alarm message	Emergency Door, Flow

Indicators	Meaning
Actual web interface alarm message	Emergency Door Opening due to Water Flow Loss (0 l/min; 36/34/35°C) (0 gal/min; 97/93/95°F) Note: The interface alarm message displays the temperatures of the top, middle, and bottom fans so you can see which temperature has been exceeded and caused the alarm to trip.
Condition	The Water Flow Loss Emergency Door Opening Temperature Threshold has been exceeded or the water flow is less than 2 l/min (.5283 gal/min).
Modules or sensors	Server Intake Temperature, Water Flow Meter
SNMP notification	Critical
Type of message	Alarm

Solution:

1. Verify water supply and verify the MCS unit is receiving water.
2. Verify that the water flow is at least 2 l/min (.5283 gal/min) or greater.
3. Verify that the Water Flow Loss Emergency Door Opening Temperature Threshold is not less than 5°C (9°F) above or more than 20°C (36°F) above the Server Intake Temperature Set Point.
4. Adjust the temperature in the Server Intake Temperature Set Point or the Water Flow Loss Emergency Door Opening Temperature Threshold fields to prevent false alarms.

IMPORTANT: Use caution when entering temperatures in the Emergency Door Opening fields. Setting the temperature thresholds too low might cause the MCS unit to shut down.

Emergency Door Opening due to High Temperature (35/36/38°C) (95/97/100°F)

Indicators	Meaning
Actual operator display alarm message	Emergency Door, Heat
Actual web interface alarm message	Emergency Door Opening due to High Temperature (35/36/38°C) (95/97/100°F) Note: The interface alarm message displays the temperatures of the top, middle, and bottom fans so you can see which temperature has been exceeded and had caused the alarm to trip.
Condition	The High Temperature Emergency Door Opening Threshold has been exceeded.
Modules or sensors	Server Intake Temperature
SNMP notification	Critical
Type of message	Alarm

Solution:

1. Verify water supply and verify the MCS unit is receiving water.
2. Verify that the High Temperature Emergency Door Opening Threshold is not less than 5°C (9°F) above or more than 20°C (36°F) above the Server Intake Temperature Set Point, or that it is not below the Water Flow Loss Emergency Door Opening Temperature Threshold.

3. Adjust the temperature in the Server Intake Temperature Set Point or the Water Flow Loss Emergency Door Opening Temperature Threshold fields to prevent false alarms.

IMPORTANT: Use caution when entering temperatures in the Emergency Door Opening fields. Setting the temperature thresholds too low might cause the MCS unit to shut down.

The condensation pump has exceeded x cycles

Indicators	Meaning
Actual operator display alarm message	Excessive Moisture
Actual web interface alarm message	The condensation pump has exceeded x cycles
Condition	The water level has exceeded the permissible level of the condensation pump sensor
Modules or sensors	Condensation pump sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Look for leaks or determine if condensation is the cause.
2. If no leaks are found, adjust the temperature in the Excessive Moisture: Condensation Pump Cycles Warning Threshold field.

IMPORTANT: Use caution when entering temperatures in the Condensation Pump Threshold fields. Be sure to determine the proper default settings to prevent false alarms, without masking problems with the MCS.

Default settings will vary, depending on the humidity level of your data center and the heat load generated by the equipment in the MCS.

The condensation pump has run more than x seconds

Indicators	Meaning
Actual operator display alarm message	Excessive Moisture
Actual web interface alarm message	The condensation pump has run more than x seconds
Condition	The water level has exceeded the permissible level of the condensation pump sensor.
Modules or sensors	Condensation pump sensor
SNMP notification	Warning
Type of message	Warning

Solution:

1. Look for leaks or determine if condensation is the cause.
2. If no leaks are found, adjust the temperature in the Excessive Moisture: Condensation Pump Running Time Warning Threshold field.

IMPORTANT: Use caution when entering temperatures in the Condensation Pump Threshold fields. Be sure to determine the proper default settings to prevent false alarms, without masking problems with the MCS.

Default settings will vary, depending on the humidity level of your data center and the heat load generated by the equipment in the MCS.

NOTE: A 24-hour clock starts when the condensation pump runs for the first time in more than 24 hours. A warning is issued if either the cycle threshold or pump running time is exceeded within the 24-hour window. The clock stops and the counters are reset to zero for warning purposes if the thresholds are not exceeded within 24 hours after the last time the condensation pump runs.

NOTE: To clear the condensation pump cycles warning, click **Cooling System** in the left navigation frame to access the Cooling System screen, and then click the **Alarms/Warnings** tab. Under the Warnings section, set Alarm Reset to **Manual** and click **Save Settings**. Then, return to the General menu and click **Clear Alarms**.

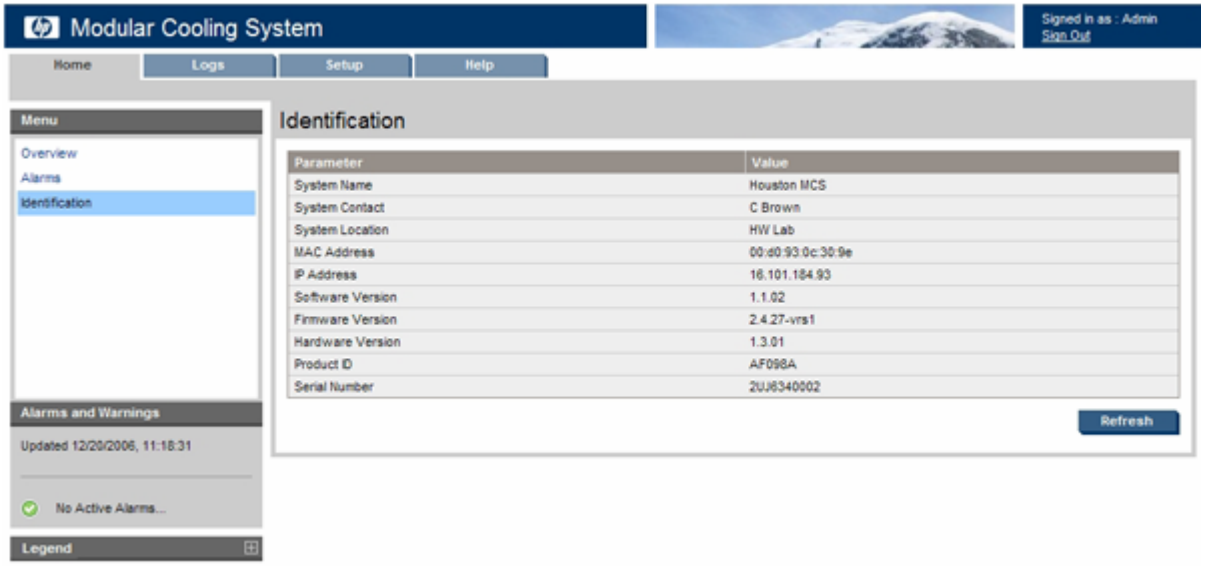
This step only clears the warning when the condensation pump is not running.

Identification menu

Click **Identification** in the left navigation frame to display the Identification screen. This screen displays specific device and contact information.

You can enter or change the system name, system contact, and system location information in the System Information tab.

You can change the IP address in the Network menu (on page 33).



Parameter	Value
System Name	Displays information entered in the Setup>Management>System Information>System Name field

Parameter	Value
System Contact	Displays information entered in the Setup>Management>System Information>System Contact field
System Location	Displays information entered in the Setup>Management>System Information>System Location field
MAC Address	Displays the MAC address
IP Address	Displays information entered in the Setup>Network>IP Address field
Software Version	Displays the software version
Firmware Version	Displays the firmware version
Hardware Version	Displays the hardware version
Product ID	Displays the product identification number
Serial number	Displays the product serial number

On the Identification screen, click **Refresh** to update the screen with current information.

Logs tab

Menu options listed under the Logs tab include:

- Alarms History menu
- Event Log menu

The Alarms History and Event Log screens display up to 150 of the most recent alarms and events. You can archive logs by periodically downloading them using FTP after FTP is enabled in the Management>Remote Access tab. The alarm.history and event.log files are located in the download directory. Every file uploaded and downloaded using FTP is recorded in the FTP.log, which is also located in the download directory. To enable FTP, see the "Remote Access tab." To view FTP Admin and FTP User privileges and assign passwords to open each account, see the "Accounts menu (on page 37)."

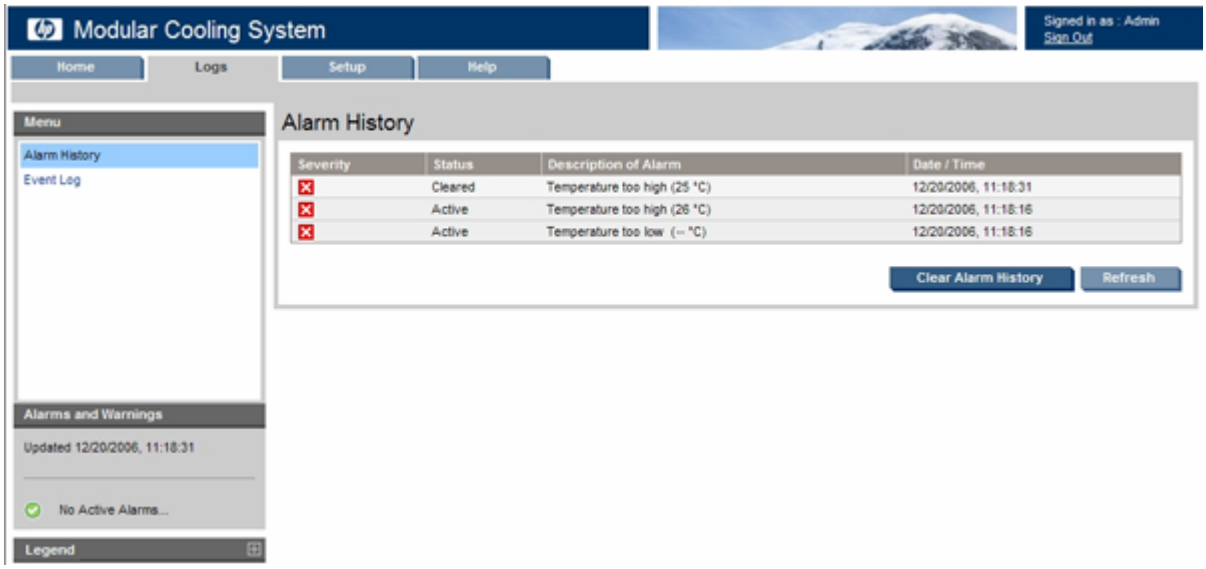
Alarm History menu

Click **Alarms History** in the left navigation frame to display the Alarm History screen. The alarms are listed by the date and time at which the alarm event most recently occurred.

The following information is displayed for each alarm:

- **Severity**—An icon indicating the severity or status of the alarm (Critical, Warning, Normal, Unknown, or Information)
- **Status**—The status of the alarm, either Active or Cleared
- **Description of Alarm**—The name of the alarm (For more information on the alarm description, see "Warning and alarm messages (on page 10).")
- **Date/Time**—The date and time at which the alarm occurred

NOTE: Under the Description of Alarm column, temperatures that display "--" in the logs are out of range.



On the Event Log screen:

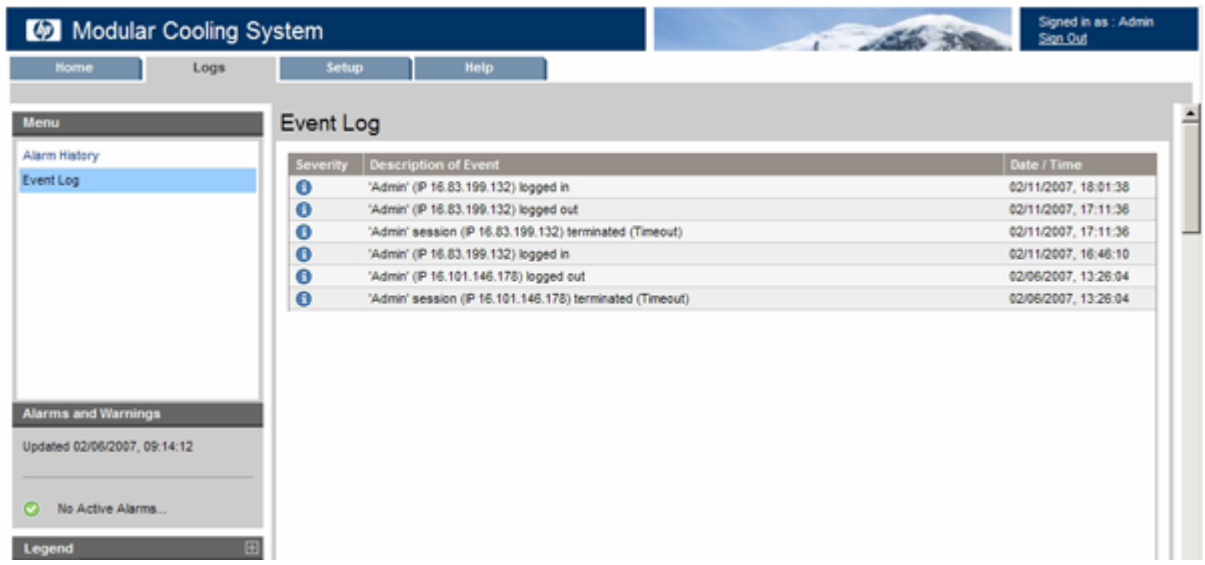
- (Admin only) Click **Clear Alarm History** to clear the log files. This function clears all of the log files, and there is no way to recover the data after it is cleared.
- Click **Refresh** to update the screen with current log information.

Event Log menu

Click **Event Log** in the left navigation frame to display the Event Log screen. The events are listed by the date and time at which the event most recently occurred.

The following information is displayed for each event:

- **Severity**—An icon indicating the severity or status of the alarm (Critical, Warning, Normal, Unknown, or Information)
- **Description of Event**—The name of the event
- **Date/Time**—The date and time at which the event occurred



On the Event Log screen:

- (Admin only) Click **Clear Event Log** to clear the log files. This function clears all of the log files, and there is no way to recover the data after it is cleared.
- Click **Refresh** to update the screen with current log information.

Setup tab

Menu options listed under the Setup tab include:

- Cooling System menu ("Cooling System" on page 23)
- General menu (on page 32)
- Network menu (on page 33)
- Management menu (on page 34)
- Accounts menu (on page 37)
- Configuration Save/Restore menu (on page 38)

These menu options enable the Admin to configure the settings for the management module. The Setup tab and all menu options are not available to User accounts.

Cooling System

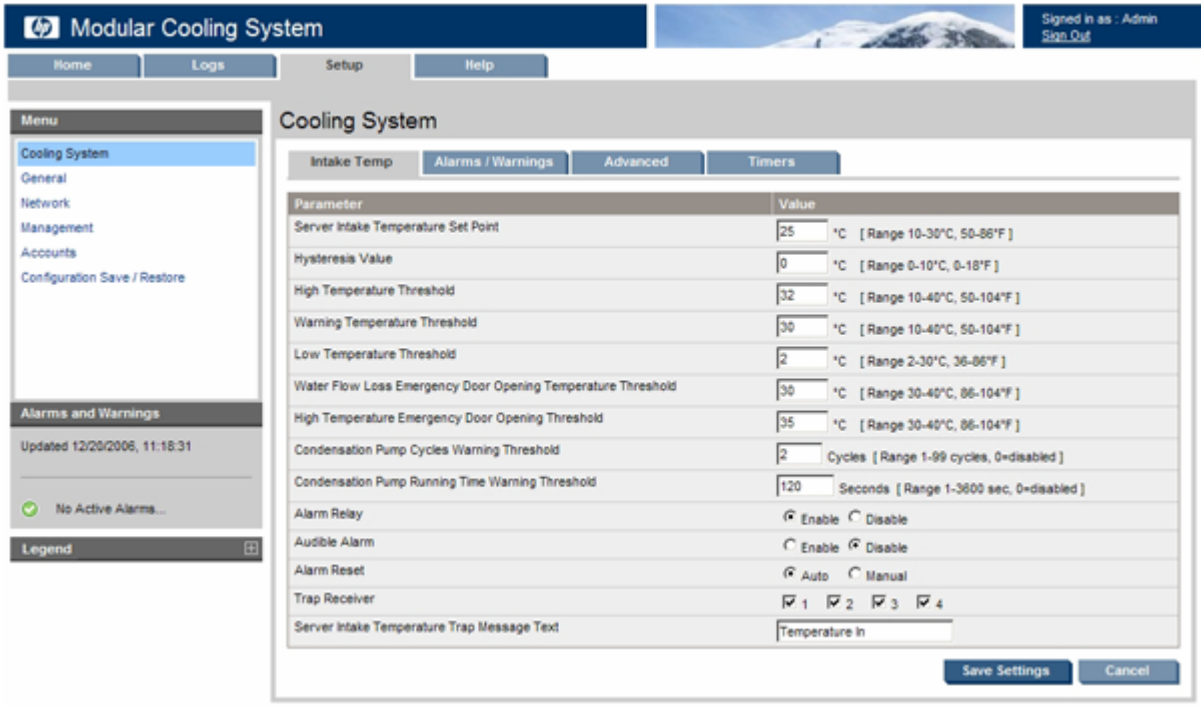
Click **Cooling System** in the left navigation frame to access the Cooling System screen. This screen enables the Admin to configure cooling system settings for the management module.

The Cooling System screen contains the following:

- Intake Temp tab (on page 24)
- Alarms/Warnings tab
- Advanced tab (on page 29)
- Timers tab

Intake Temp tab

This screen enables the Admin to change server intake temperature settings for the management module.



To change the server intake temperature settings:

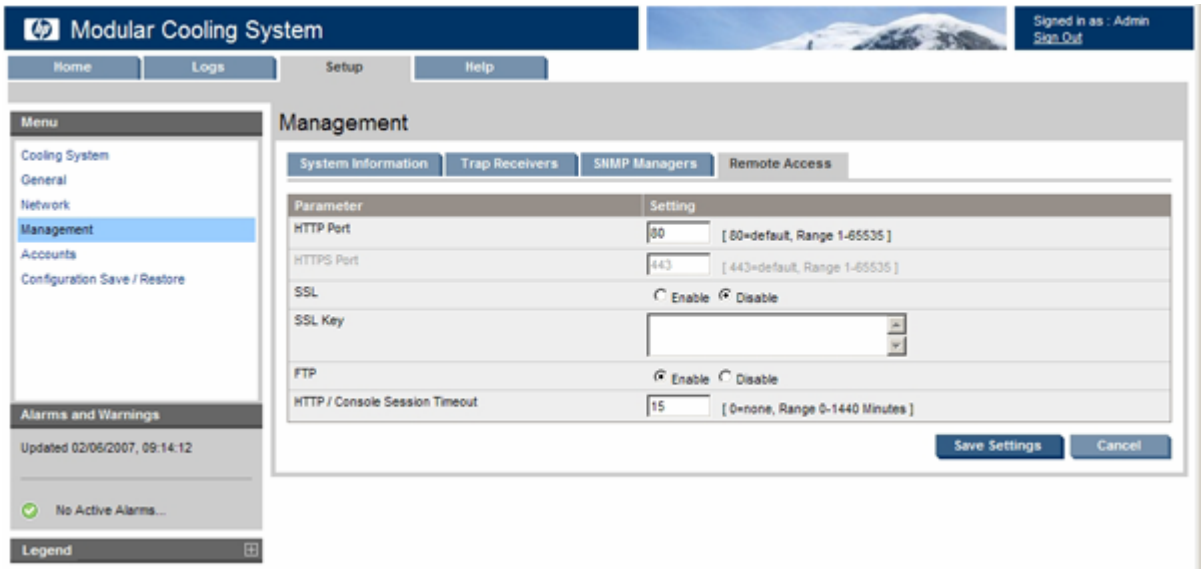
1. Enter a server intake temperature set point in the Server Intake Temperature Set Point field.
2. Enter a temperature range in which the server intake temperature can vary in the Hysteresis Value field.
3. Enter a maximum air temperature at which a critical alarm is issued and a trap is sent if the server intake temperature is exceeded for the High Temperature Threshold field.
4. Enter an air temperature at which a warning is issued and a trap is sent if the server intake temperature is exceeded for the Warning Temperature Threshold field.
5. Enter an air temperature at which an alarm is issued and a trap is sent if the server intake temperature drops below for the Low Temperature Threshold field.
6. Enter an air temperature at which an alarm is issued and a trap is sent if the server intake temperature is exceeded for the Water Flow Loss Emergency Door Opening Temperature Threshold field.
7. Enter an air temperature at which an alarm is issued and a trap is sent if the server intake temperature is exceeded for the High Temperature Emergency Door Opening Threshold field.
8. Enter an air temperature at which an alarm is issued and a trap is sent if the condensation pump cycles are exceeded for the Excessive Moisture: Condensation Pump Cycles Warning Threshold.
9. Enter an air temperature at which an alarm is issued and a trap is sent if the condensation pump running time is exceeded for the Excessive Moisture: Condensation Pump Running Time Warning Threshold.

NOTE: A 24-hour clock starts when the condensation pump runs for the first time in more than 24 hours. A warning is issued if either the cycle threshold or pump running time is exceeded within the 24-hour window. The clock stops and the counters are reset to zero for warning purposes if the thresholds are not exceeded within 24 hours after the last time the condensation pump runs.

10. Select to enable or disable the alarm relay from the Alarm Relay radio buttons. This setting is only for the Server Intake Temperature.
    - Select **Enable** to allow the alarm relay when a temperature alarm is generated.
    - Select **Disable** to not allow the alarm relay when a temperature alarm is generated.
11. Select to enable or disable the audible alarm from the Audible Alarm radio buttons. This setting is only for the Server Intake Temperature.
    - Select **Enable** to allow the audible alarm to sound when a temperature alarm is generated.
    - Select **Disable** to not allow the audible alarm to sound when a temperature alarm is generated.
12. Select to enable the alarm to be reset (which also resets the audible alarm and alarm relay) automatically (Auto) or manually (Manual) from the Alarm Reset radio buttons. This setting is only for the Server Intake Temperature.
    - Select **Auto** to allow the alarm to be turned off automatically if the temperature returns to a valid range after a temperature alarm is generated. This will terminate the audible alarm.
    - Select **Manual** to allow the alarm to be turned off by clicking Clear Alarms in the Setup>General menu. The alarm can also be cleared by pressing the C key on the management module after any alarm is generated.
13. Select the checkbox to activate trap receivers 1 through 4.
14. Enter information that displays when a server intake temperature trap is received in the Server Intake Temperature Trap Message Text field.
15. Do one of the following:
    - Click **Save Settings** to save the information.
    - Click **Cancel** to undo the changes.

Remote Access tab

This screen enables the Admin to enter information for remote access to the management module.



To enable SSL:

1. Select to enable SSL using the SSL radio button.
2. Click **Save Settings.** A new HTTPS URL appears on the operator display.
3. Log in to the web interface using the new IP address or hostname (using the `https://`*hostname[:port number]* format).
4. Enter the port number to use HTTPS in the HTTPS Port field.

   A default self-signed SSL certificate can be used, or you can enter your own certificate. The default certificate is used if another certificate is not entered.

   You can also enter your own SSL and private keys in the following format:

   ```
   -----BEGIN CERTIFICATE-----
   MIICgj......
   .....
   ......Qorw==
   -----END CERTIFICATE-----
   -----BEGIN RSA PRIVATE KEY-----
   MIICXAIB......
   .....
   ....tFlYw=
   -----END RSA PRIVATE KEY-----
   ```
5. Click **Save Settings.**
6. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

To disable SSL:

1. Select to disable SSL using the SSL radio button.

2. Enter the port number to use HTTP in the HTTP Port field.
3. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

To configure other remote access settings:

1. Select to enable or disable FTP using the FTP radio buttons.
2. Enter the number of minutes for the HTTP/Console Session Timeout field. The default is 30 minutes.
3. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

Browser security alert

Secure browsing requires the use of SSL. SSL is a protocol layer that lies between HTTP and TCP that provides secure communication between a server and a client and is designed to provide privacy and message integrity. SSL is commonly used in web-based transactions to authenticate the web server, which indisputably identifies the server to the browser. SSL also provides an encrypted channel of communication between the server and the browser. The encrypted channel ensures integrity of the data between the web server and the browser, so that data can neither be viewed nor modified while in transit. The management module uses a system generated and unique key.

An integral part of SSL is a security certificate, which identifies the management module. If your browser displays a security alert when browsing to the management module, it can be for one of several reasons:

- The certificate is untrusted, meaning it was signed by a certifying authority that is unknown to your browser.
- The certificate has expired or is not yet valid. This condition can occur if you issue your own certificate and it has expired.
- The name on the certificate does not match the name of the site in the browser address field.

For more information about security considerations, see "Security considerations overview (on page 52)."

Establishing a secure session for Internet Explorer

The first time you browse to the management module, the Secure Session screen appears. To ensure a secure connection, verify that you are browsing to the desired management module:

1. Click **View Certificate.**
2. Verify that the name in the Issued To field is the name of your management module.
3. Perform any other steps necessary to verify the identity of the management module.

> △ **CAUTION:** If you are not sure this is the desired management module, do not proceed. Importing a certificate from an unauthorized source relays your login credentials to that unauthorized source. Exit the certificate window and contact the system administrator.

After verifying the management module, do one of the following:

- Import the certificate and proceed.
  a. Click **View Certificate.** The certificate appears.
  b. Click **Install Certificate.** The Certificate Import wizard runs.

c. Click **Next.** The Certificate Store screen appears.
d. Select **Automatically select the certificate store based on the type of certificate,** and click **Next.**
e. Click **Finish.** A message appears, asking for verification of the root store.
f. Click **Yes.**

- Proceed without importing the certificate by clicking **Yes** at the Security Alert window. You continue to receive the Security Alert each time you log in until you import the certificate. Your data is still encrypted.
- Exit and import the certificate into your browser from a file provided by the administrator.
  a. Click **No** at the Security Alert window.
  b. Obtain an exported certificate file from the administrator.

> **NOTE:** If using Internet Explorer, you can manually import the file into the browser by clicking **Tools>Internet Options>Content>Certificates>Import**.

Establishing a secure session for Mozilla

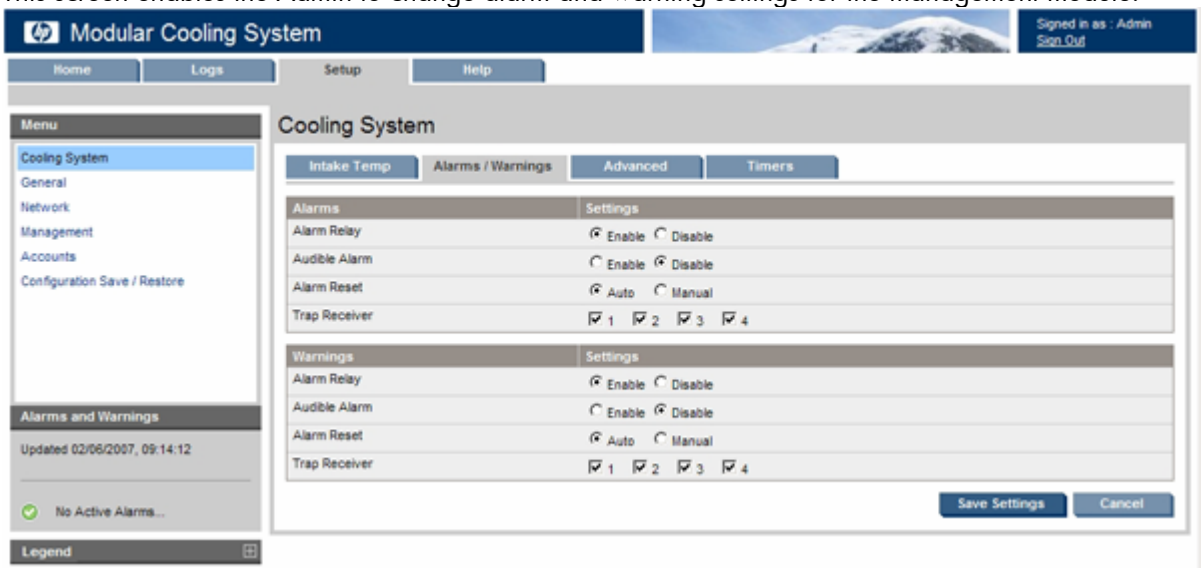
The first time you browse to the management module, the Secure Session screen appears. To ensure a secure connection, verify that you are browsing to the desired management module:

1. Click **Examine Certificate.**
2. Verify that the name in the Issued To field is the name or IP address of your management module.
3. Perform any other steps necessary to verify the identity of the management module.
4. After verifying the management module, do one of the following:
   a. Click either **Accept this certificate permanently** or **Accept this certificate temporarily for this session.**
   b. Click **OK.**

> **NOTE:** If using Mozilla, you can manually import the file into the browser by clicking **File>Preferences>Certificates>Privacy & Security>Manage Certificates>Authorities>Import**.

Alarms/Warnings tab

This screen enables the Admin to change alarm and warning settings for the management module.



To change the alarm and warning settings:

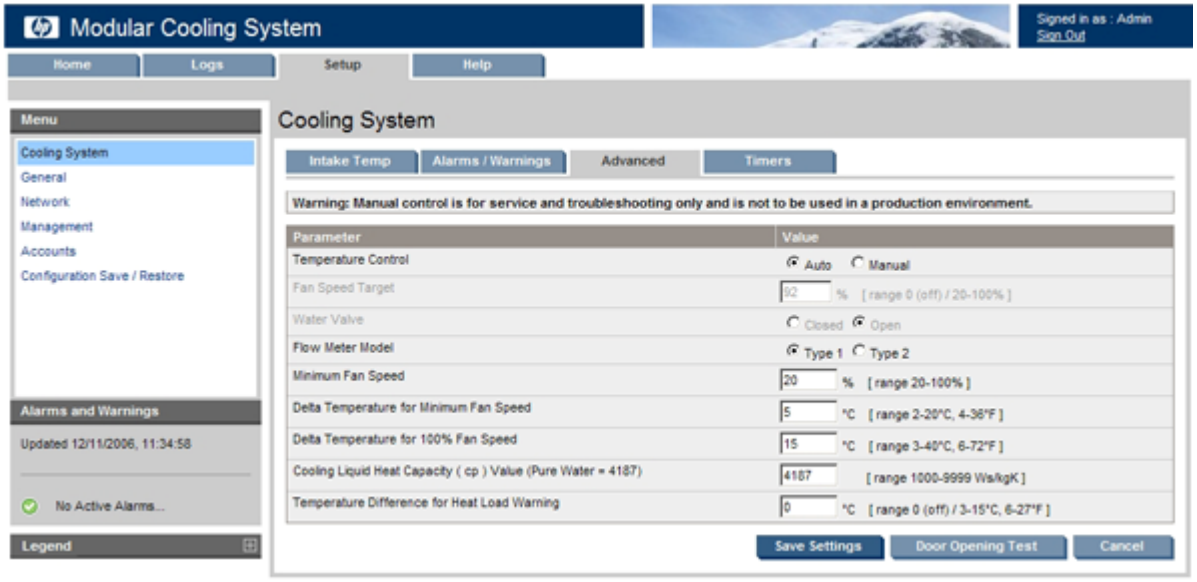
1. Select to enable or disable the alarm relay from the Alarm Relay radio buttons. This setting affects all alarms and warnings, except for the Server Intake Temperature.
   - Select **Enable** to allow the alarm relay when a temperature alarm is generated.
   - Select **Disable** to not allow the alarm relay when a temperature alarm is generated.
2. Select to enable or disable the audible alarm from the Audible Alarm radio buttons. This setting affects all alarms and warnings, except for the Server Intake Temperature.
   - Select **Enable** to allow the audible alarm to sound when an alarm is generated.
   - Select **Disable** to not allow the audible alarm to sound when an alarm is generated.
3. Select to allow the alarm to be reset (which also resets the audible alarm and alarm relay) automatically (Auto) or manually (Manual) from the Alarm Reset radio buttons. This setting affects all alarms and warnings, except for the Server Intake Temperature.
   - Select **Auto** to allow the alarm to be turned off automatically if the condition returns to a valid range after an alarm is generated.
   - Select **Manual** to allow the alarm to be turned off by clicking Clear Alarms in the Setup>General menu. The alarm can also be cleared by pressing the **C** key on the management module after any alarm is generated.
4. Select the checkbox to deactivate the scheduled alarms for trap receivers 1 through 4.
5. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

Advanced tab

This screen contains the Temperature Difference for Heat Load Warning field. This field is used to adjust the heat load temperature which is the temperature difference between the highest and lowest Server Exhaust Temperature. If the heat load temperature difference varies by more than this setting then a Heat

load? warning appears in the operator display, and a Heat Load Warning appears in the web interface. Setting the value to 0 disables the warning.

When the MCS unit is in Auto mode, the Fan Speed Target and Water Valve fields are not available.



On the Advanced screen, the administrator can change the temperature control modes for the management module.

IMPORTANT: Temperature Control Manual mode is for service and troubleshooting only and is not to be used in a production environment.

- Temperature Control Auto mode—Used for operating the MCS unit after a satisfactory water flow rate has been obtained.

  In this mode, the MCS unit operates automatically, according to the settings you have assigned to the following parameters:

  - Flow Meter Model

    NOTE: If you have the Type 2 flow meter, your MCS unit will have a label on the inside of the back door. For more information on the flow meter model label, see the *HP Modular Cooling System User Guide*.

  - Minimum Fan Speed
  - Delta Temperature For Minimum Fan Speed
  - Delta Temperature For 100% Fan Speed
  - Cooling Liquid Heat Capacity
- Temperature Control Manual mode—Used to verify the water flow rate after the cold water supply has been connected. When the water flow rate has been validated, use the Auto mode setting.

  In this mode, the MCS unit operates, manually, according to the settings you have assigned to the following parameters:

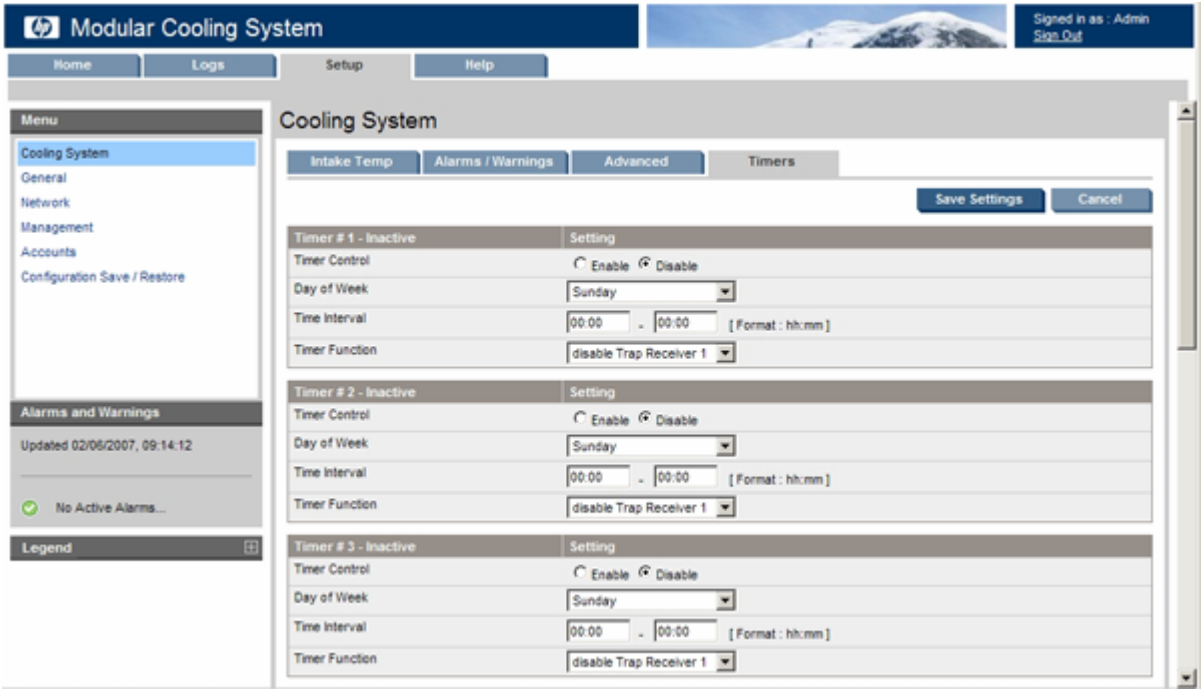
  - Fan Speed Target
  - Water Valve State

After you change the temperature control modes, you can do the following:

- Click **Save Settings** to save the information
- Click **Door Opening Test** to open the MCS front and rear doors and test the magnetic locks.
- Click **Cancel** to undo the changes.

Timers tab

This screen enables the Admin to change timer settings for the management module. Timers are used to disable particular trap receivers on different days at different times of the week.

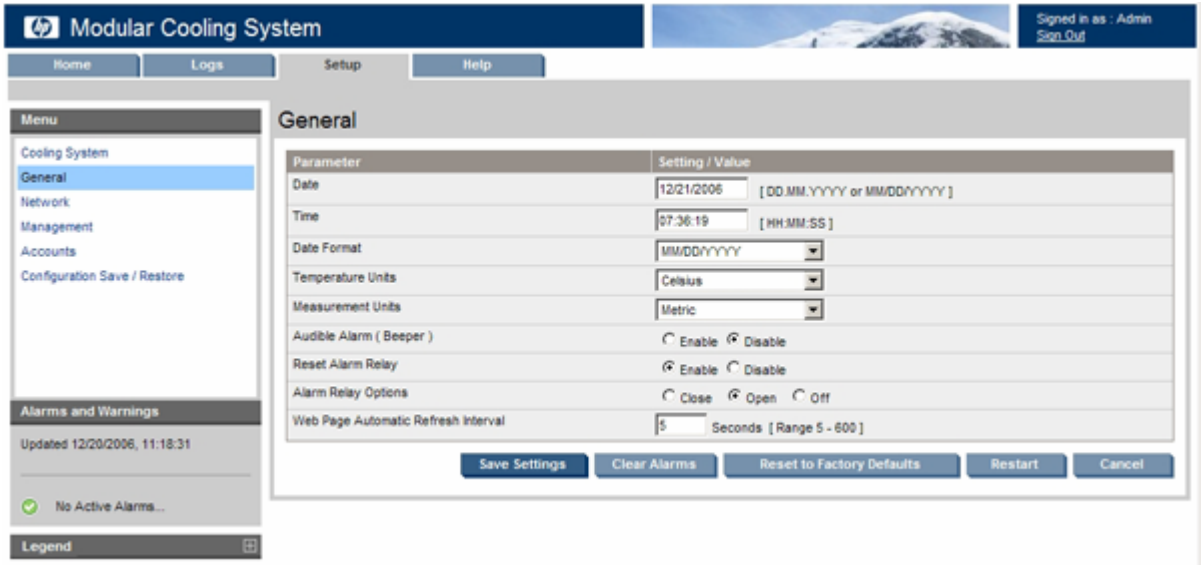


To change the timer settings:

1. Select to enable or disable the timer control from the Timer Control radio buttons.
2. Select a day of the week from the Day of Week dropdown box.
3. Enter a time interval in the Time Interval field.
4. Select a timer function from the Timer Function dropdown box.
5. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

General menu

Click **General** in the left navigation frame to display the General screen. This screen enables the Admin to configure general management module parameters.



To change the general parameters:

1. Enter a date in the Date field. (If NTP is enabled in the Network menu, do not enter a date in this field.)
2. Enter a time in the Time field. (If NTP is enabled in the Network menu, do not enter a date in this field.)
3. Select a date format from the Date Format dropdown box. Use MM/DD/YYYY for U.S. date format and DD.MM.YYYY for Euro/World format.
4. Select a temperature unit from the Temperature Units dropdown box.
5. Select a measurement unit from the Measurement Units dropdown box.
6. Select to enable or disable the audible alarm from the Audible Alarm (Beeper) radio buttons.
   - Select **Enable** to allow the audible alarm to sound when an alarm is generated.
   - Select **Disable** to not allow the audible alarm to sound when an alarm is generated.
7. Select to enable or disable the reset alarm relay function in the Alarms/Warnings tab, using the Alarm Relay Options radio buttons.
   - Select **Enable** to allow the alarm relay function when an alarm is generated.
   - Select **Disable** to not allow the alarm relay function when an alarm is generated.
8. Select to close, open, or turn off the alarm relay options from the Alarm Relay Options radio buttons.
   - Select **Close** so that the alarm relay disconnects a circuit (normally closed) upon alarm activation.
   - Select **Open** so that the alarm relay completes a circuit (normally open) upon alarm activation.
   - Select **Off** so that the alarm relay is not activated (normally open) upon alarm activation.
9. Enter a range for the web page automatic refresh interval in the Web Page Automatic Refresh Interval field.
10. Do one of the following:
    - Click **Save Settings** to save the information.

- Click **Clear Alarms** to clear the alarms.

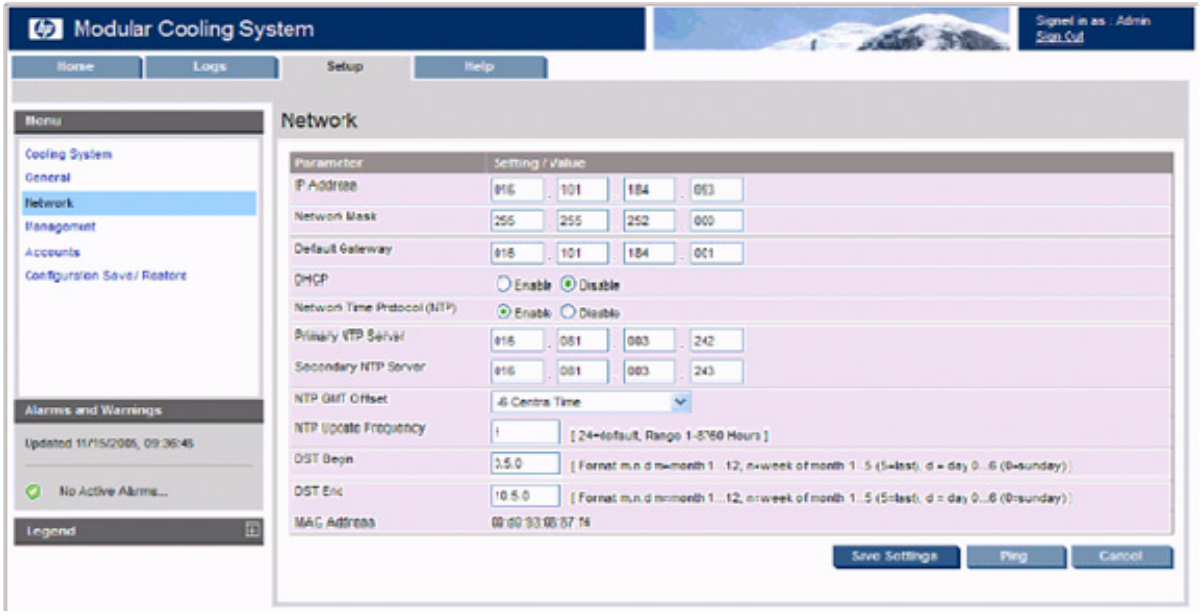
  NOTE: To clear the condensation pump cycles warning, click **Cooling System** in the left navigation frame to access the Cooling System screen, and then click the **Alarms/Warnings** tab. Under the Warnings section, set Alarm Reset to **Manual** and click **Save Settings**. Then, return to the General menu and click **Clear Alarms**.

  This step only clears the warning when the condensation pump is not running.

11. Click **Reset to Factory Defaults** to reset the parameters to the defaults set by the factory. You are prompted to reboot.
    - Click **Restart** to restart the management module.
    - Click **Cancel** to undo the changes.

Network menu

Click **Network** in the left navigation frame to access the Network screen. This screen enables the Admin to configure network settings for the management module.



To set a static IP:

1. Disable DHCP (by default, DHCP is enabled) using the DHCP radio button.
2. Click **Save Settings.**
3. Change the IP address in the IP Address field of the management module.
4. Change the network mask of the management module.
5. Change the default gateway of the management module.
6. Click **Save Settings.**
7. Log in to the web interface using the new IP address or hostname.
8. Continue to the next section.

To configure the network settings:

NOTE: When DHCP is enabled, the IP Address, Network Mask, and Default Gateway fields are not available.

1. Select to enable or disable NTP from the Network Time Protocol (NTP) radio buttons.
2. If you enable NTP:
   a. Enter the IP address of the primary NTP server in the Primary NTP Server field.
   b. Enter the IP address of the secondary NTP server in the Secondary NTP Server field.

      NOTE: If NTP is not enabled, selecting a time zone from the NTP GMT Offset dropdown box changes the system clock by the hours offset.

   c. Select the time zone from the NTP GMT Offset dropdown box.
   d. Enter the number of hours that should pass between each date and time update in the NTP Update Frequency field.
   e. Proceed to step 4.
3. If you do not enable NTP:
   a. Enter the date in the Date field on the General menu (on page 32).
   b. Enter the time in the Time field on the General menu (on page 32).
   c. Enter the date for DST to begin in the DST Begin field.
   d. Enter the date for DST to end in the DST End field.
   e. Proceed to step 4.
4. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

Click **Ping** to test the network connectivity to another device IP address.

Management menu

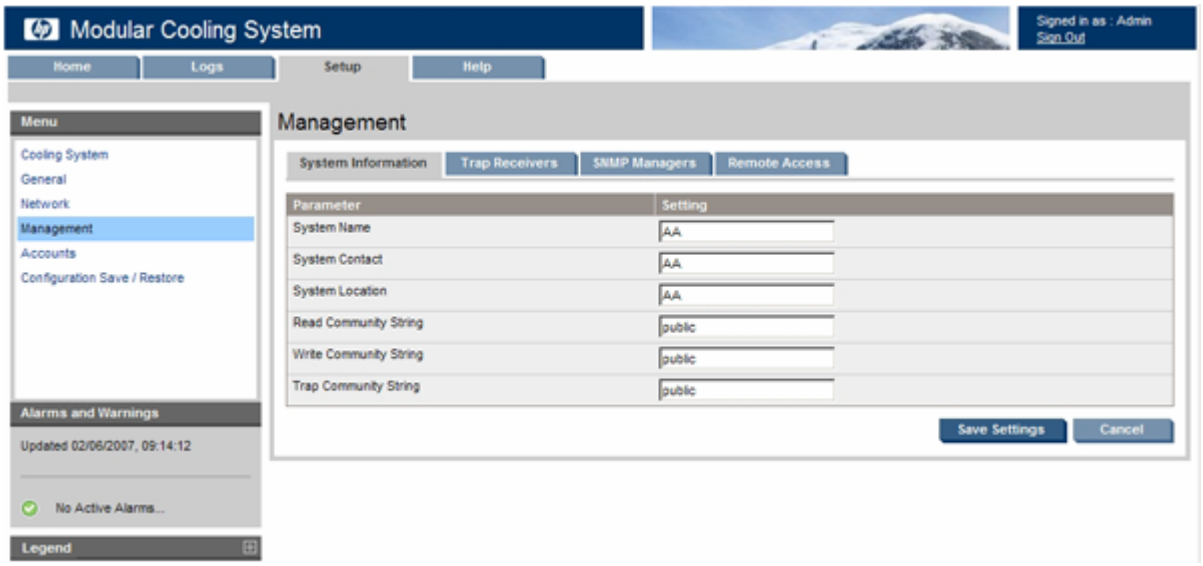
Click **Management** in the left navigation frame to access the Management screen. This screen enables the Admin to configure network management settings for the management module.

The Management screen contains the following:

- System Information tab
- Trap Receivers tab (on page 35)
- SNMP Managers tab
- Remote Access tab

System Information tab

This screen enables the Admin to enter contact information for the management module. The information entered on this screen appears on the Identification screen and is included with SNMP traps sent by the management module.



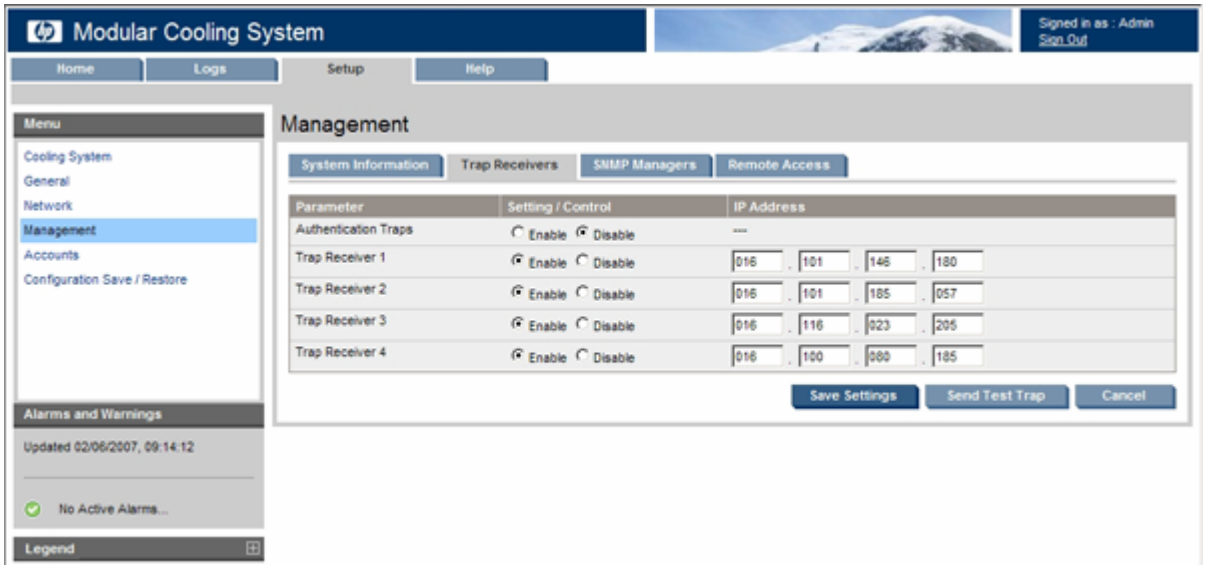
To enter the contact information:

1. Enter the name of the management module in the System Name field.
2. Enter the name of the contact person in the System Contact field.
3. Enter the name of the location in the System Location field.
4. Enter the Read community string.
5. Enter the Write community string.
6. Enter the Trap community string.
7. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

Trap Receivers tab

This screen enables the Admin to enter information for servers that should receive SNMP traps from the management module.

To receive traps in HP SIM, see "Systems Insight Manager integration (on page 49)."



To configure which servers should receive traps:

1. Select to enable or disable SNMP authentication traps from the Authentication Traps radio buttons.
2. Select to enable up to four SNMP traps from the Trap Receivers 1 through 4 radio buttons.
3. Enter the IP address for up to four trap recipients in the IP Address fields.
4. To save the settings, choose one of the following options:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.
5. Click **Send Test Trap** to send a test SNMP trap to all enabled trap receivers.

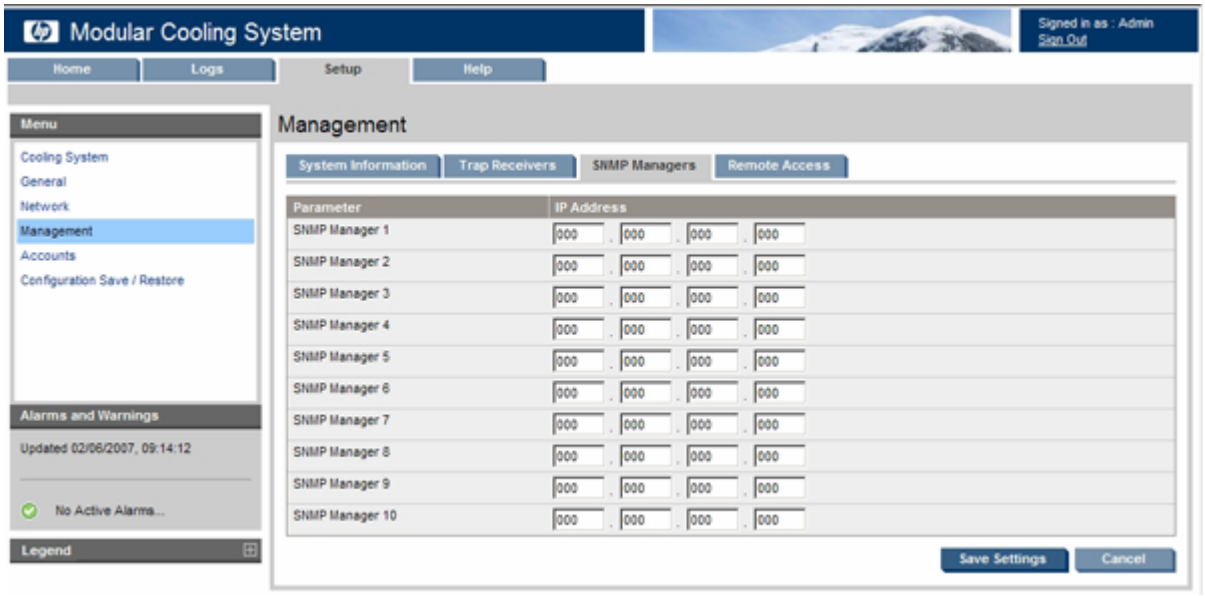
SNMP Managers tab

This screen enables the Admin to enter information for SNMP managers. SNMP managers are computers that use the MIB to request information and understand traps from the management module.

If all IP addresses are 0.0.0.0, all SNMP managers are allowed to request information from the module.

If one or more of the SNMP managers have an IP address, only those SNMP managers are allowed to request SNMP information.

The SNMP manager entries do not have any effect on sending traps.



To configure SNMP managers:

1. Enter the IP address for each SNMP manager in the IP Address field.
2. Do one of the following:
   - Click **Save Settings** to save the information.
   - Click **Cancel** to undo the changes.

Accounts menu

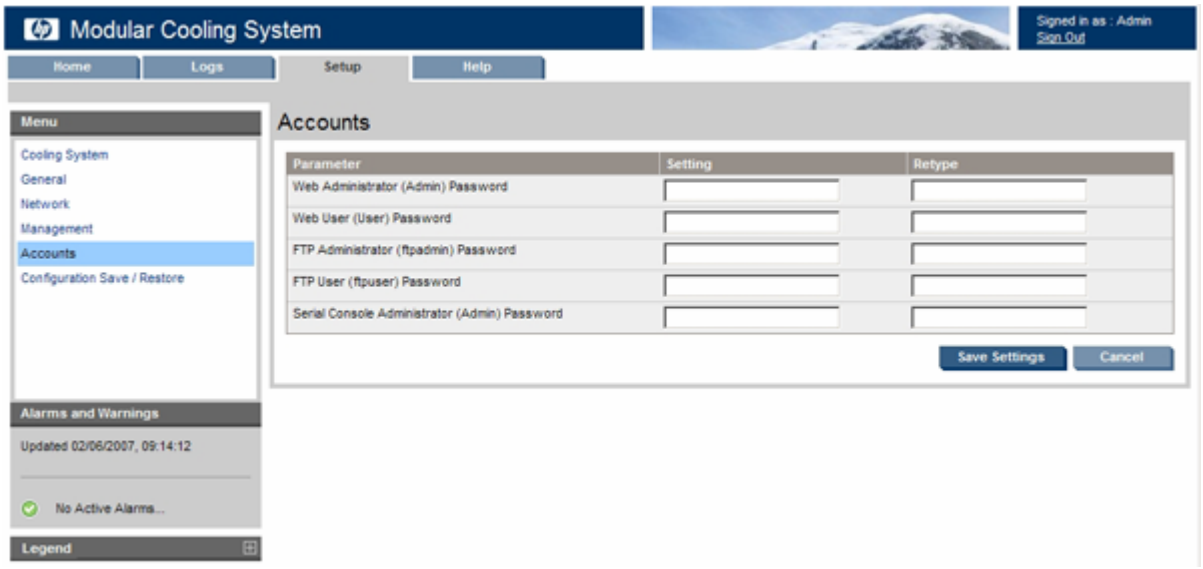
Click **Accounts** in the left navigation frame to access the Accounts screen. This screen enables the Admin to modify web and FTP Admin and User passwords and Serial Console Admin passwords.

FTP Admin and FTP User accounts are blocked until the Admin resets the management module settings so that FTP is enabled in the Management>Remote Access tab, and assigns a password to open each account. The Web User account is also blocked until the Admin assigns a password to open the account.

The following user accounts have these privileges:

- Web Administrator (Admin)—Has Admin privileges
- Web User (User)—Has read-only privileges
- FTP Administrator (ftpadmin)—Has limited privileges, such as uploading, downloading, and deleting log files
- FTP User (ftpuser)—Has limited privileges, such as downloading log files

- Serial Console Administrator (Admin)—Has full privileges to all of the serial console menu items



To modify a password:

1. Enter the new password in the Setting field.
2. Enter the new password again in the Retype field.
3. Do one of the following:
   - Click **Save Settings** to save the updated account information.
   - Click **Cancel** to undo the changes.

Configuration Save/Restore menu

Click **Configurations Save/Restore** in the left navigation frame to access the Configuration Save/Restore screen. This screen enables the Admin to save and restore a configuration file.

On the Configuration Save/Restore screen:

- Click **Save Configuration** to save the configuration file.

- Click **Restore Configuration** to restore the configuration file.
- Click **Undo Changes** to undo the changes.

You can save the configuration and then restore the same configuration on multiple management modules. The IP address must be set individually on each unit through DHCP or the serial interface before the replication can be performed.

To replicate a configuration to multiple MCS units, save the configuration file:

1. Configure the settings through the web interface.
2. From the Setup tab (on page 23), select **Configuration Save/Restore.**
3. Click **Save Configuration.** Browse to where you want to save the configuration file.

To restore the saved configuration file:

> **NOTE:** Restore only configuration files that have been saved from a MCS unit.

1. At the new unit where you want to restore the configuration file, set the IP address through the serial interface.

   -or-

   If the IP address is DHCP assigned, the IP address is available from the operator display.
2. Log in to the web interface.
3. From the Setup tab (on page 23), select **Configuration Save/Restore.**
4. Browse to where you saved the configuration file.
5. Click **Restore Configuration.** You are prompted to restart the management module. Do not restart until you verify or change the network settings.
6. Select to enable or disable DHCP (enabled is the default setting) from the DHCP radio buttons.
7. Set a static IP. For more information, see "Network menu (on page 33)."
8. Reboot the management module.

Help tab

Menu options listed under the Help tab include:

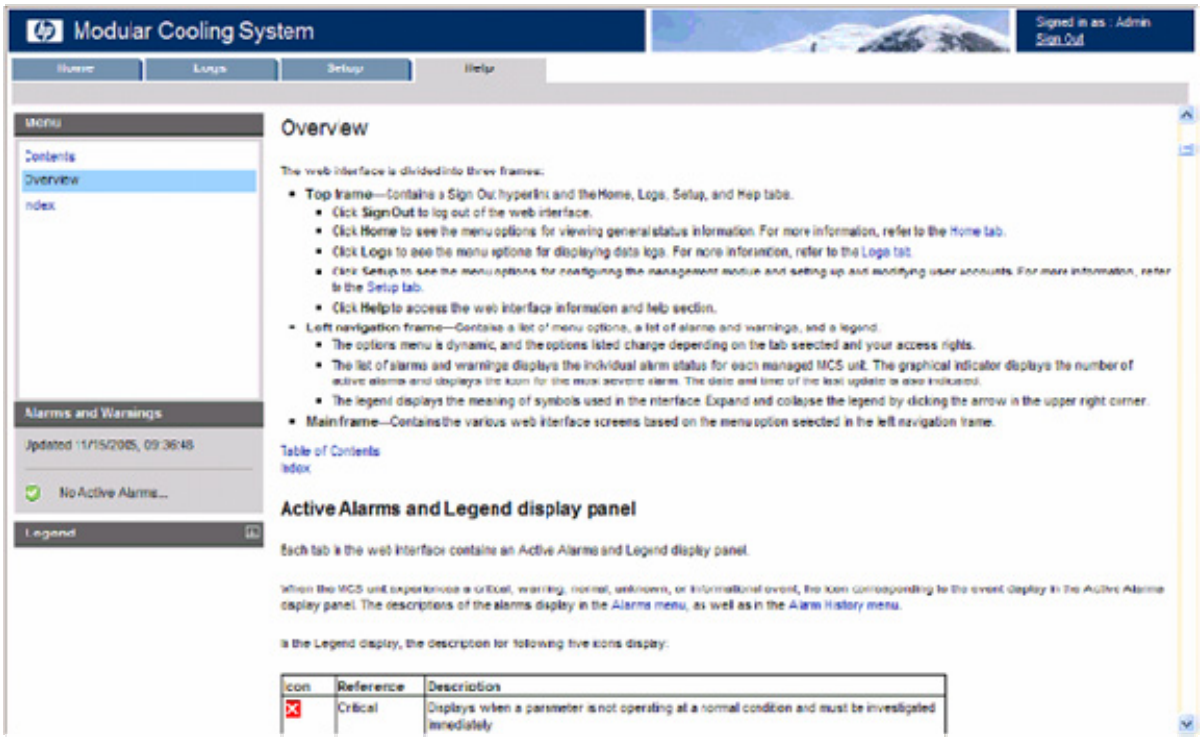
- Contents menu (on page 40)
- Overview page (on page 41)
- Index menu (on page 42)

Contents menu

Click **Contents** in the left navigation frame to display the Contents menu. This menu provides a list of the links to help topics.

Overview page

Click **Overview** in the left navigation frame to display the Overview page. This page displays overview information about the product.



Index menu

Click **Index** in the left navigation frame to display the Index menu. This menu provides a list of the links to help topics.

Upgrading the firmware

In this section

Upgrading the HP Modular Cooling System firmware

The MCS unit must have the latest firmware to work properly.

To upgrade the firmware:

1. Access the HP website (http://www.hp.com).
2. Click **Software & Driver Downloads**.
3. Ensure that the Download drivers and software (and firmware) option is selected.
4. Type `Modular Cooling System` in the product name field, and then click **Search**.

If any firmware upgrades are available, they will display on this page.

Instructions to perform the upgrade are included in the download pack.

Cooling performance parameter settings

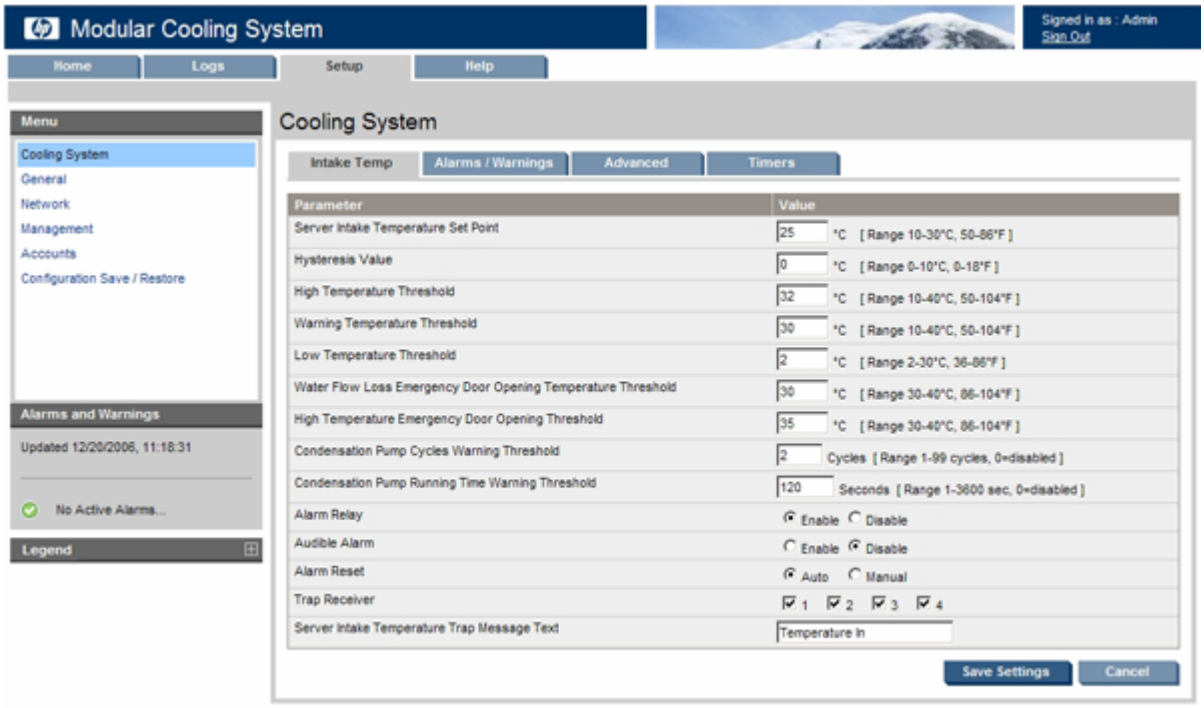
In this section

Cooling performance parameter settings overview

The MCS unit has several cooling performance parameter settings. These settings control the fan speed and water flow to meet the rack-mounted component's cooling needs.

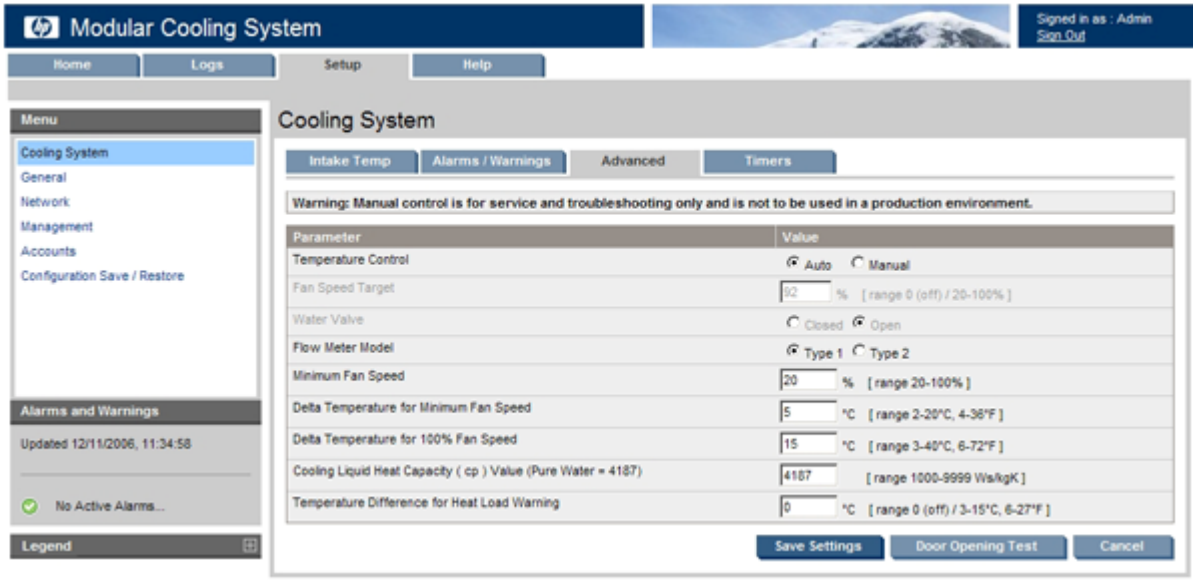
The temperature of the server intake air is constantly controlled by the opening and closing of the solenoid actuated water valve inside the MCS unit. When the server intake air temperature goes above the Server Intake Temperature Set Point the water valve opens. When the server intake air temperature falls below the Server Intake Temperature Set Point minus the Hysteresis Value, the water valve closes.

The speed of the fan units is constantly controlled through the control system using the server intake and server exhaust temperatures.



Parameter	Function
Server Intake Temperature Set Point	Used to control the desired air temperature going into the front of the servers
Hysteresis Value	Used to control the server intake temperature range and optimize the water valve cycle frequency
High Temperature Threshold	Used to issue a Critical alarm if the high temperature threshold temperature is exceeded

Parameter	Function
Warning Temperature Threshold	Used to issue a warning if the warning temperature threshold temperature is exceeded
Low Temperature Threshold	Used to issue a warning if the low temperature threshold temperature is exceeded
Water Flow Loss Emergency Door Opening Temperature Threshold	Used to open the MCS doors when the temperature threshold is exceeded and water loss is detected This value cannot be lower than 5°C (9°F) above or more than 20°C (36°F) above the Server Intake Temperature Set Point.
High Temperature Emergency Door Opening Threshold	Used to open the MCS doors when the temperature threshold is exceeded This value: • Cannot be lower than 5°C (9°F) above or more than 20°C (36°F) above the Server Intake Temperature Set Point. • Cannot be less than the Water Flow Loss Emergency Door Opening Temperature Threshold.
Excessive Moisture: Condensation Pump Cycles Warning Threshold	Used to issue a warning if the condensation pump exceeds the permissible number of cycles within a 24-hour period
Excessive Moisture: Condensation Pump Running Time Warning Threshold	Used to issue a warning if the condensation pump has run longer than the permissible running time
Alarm Relay	Used to enable or disable the alarm relay
Audible Alarm	Used to enable or disable the audible alarm
Alarm Reset	Used to enable the alarm to be reset automatically (Auto) or manually (Manual)
Trap Receiver	Used to activate trap receivers 1 through 4
Server Intake Temperature Trap Message Text	Used to enter information that displays when a server intake temperature trap is received



IMPORTANT: Temperature Control Manual mode is for service and troubleshooting only and is not to be used in a production environment.

Parameter	Function
Temperature Control	Used in Auto mode to determine if the MCS unit operates in Auto mode or Manual mode
Fan Speed Target	Used in Manual mode to increase or decrease the fan speed
Water Valve	Used in Manual mode to close or open the water valve in Manual mode
Flow Meter Model	Used in Auto mode to select the water flow meter that is installed in the MCS
Minimum Fan Speed	Used in Auto mode to set the lowest fan speed in Auto mode
Delta Temperature for Minimum Fan Speed	Used in Auto mode to set the maximum delta temperature when the Minimum Fan Speed will be used
Delta Temperature for 100% Fan Speed	Used in Auto mode to set the minimum delta temperature when the 100% Fan Speed will be used
Cooling Liquid Heat Capacity (Cw) Value	Used in Auto mode to calculate the energy extracted by the air to water heat exchanger unit (This value for pure water is 4,187 Ws/kg and can be a lower value if additives are included in the water.)

Delta temperature (Server Intake Temp/Server Exhaust Temp)

Delta temperature is calculated from the temperature difference between the server intake temperature and server exhaust temperature. The server intake temperature, or cold air, is the air coming from the heat exchanger units and pushed through the fan units. The server exhaust temperature, or hot air, is the air coming from the fan units and being pushed through the heat exchanger units.

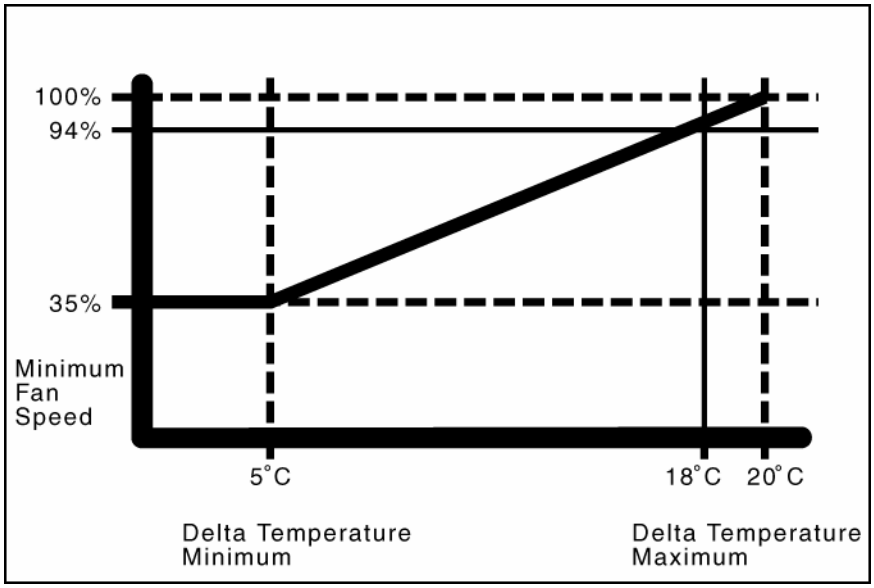
Example

	Server intake temperature	Server exhaust temperature
Top	24.5°C (76.1°F)	38.8°C (101.8°F)
Middle	24.8°C (76.6°F)	39.1°C (102.4°F)
Bottom	25.1°C (77.2°F)	40.3°C (104.5°F)
Average	24.8°C (76.6°F)	39.4°C (102.9°F)

Cooling air flow supplied by the MCS unit

Delta temperature is used to determine and control the speed of the rotating fans.

This example shows the fan speed control function when the minimum fan speed is 35%, delta temperature for minimum fan speed is 5°C (9°F), the delta temperature for 100% fan speed is 20°C (36°F). In this case, the delta control temperature is 18°C (32°F) and will cause the fans to run at 94% speed.



Adjusting the cooling air flow provided by the MCS unit

To adjust the cooling air flow provided by the MCS unit while in Temperature Control Auto mode:

1. Click the **Setup** tab (on page 23), and then click the **Advanced** tab (on page 29).
2. Enter a Minimum Fan Speed.
3. Enter a Delta Temperature For Minimum Fan Speed.
4. Enter a Delta Temperature 100% Fan Speed.

Server intake temperature provided by the MCS unit

The management module constantly compares the server intake temperature to the range calculated from the Server Intake Temperature Set Point and the Hysteresis value.

- If the server intake temperature is above the Server Intake Temperature Set Point, the water valve opens (if not already opened) and cold water enters the heat exchanger units.
- If the server intake temperature is below or equal to the Server Intake Temperature Set Point minus the Hysteresis value, the water valve closes (if not already closed).
- If the server intake temperature is between the Hysteresis value, the water valve remains unchanged from its previous state.

Setting and controlling the server intake temperature

To adjust the Server Intake Temperature:

1. Click the **Setup** tab (on page 23), click the **Intake Temp** tab (on page 24), and enter a Server Intake Temperature Set Point.
2. In the same tab, enter a Hysteresis value. Start with a 2°C (3.6°F) difference.

Temperature Control settings

On the Advanced screen, the administrator can change the temperature control modes for the management module.

IMPORTANT: Temperature Control Manual mode is for service and troubleshooting only and is not to be used in a production environment.

- Temperature Control Auto mode—Used for operating the MCS unit after a satisfactory water flow rate has been obtained.

  In this mode, the MCS unit operates automatically, according to the settings you have assigned to the following parameters:

  - Flow Meter Model

    NOTE: If you have the Type 2 flow meter, your MCS unit will have a label on the inside of the back door. For more information on the flow meter model label, see the *HP Modular Cooling System User Guide*.

  - Minimum Fan Speed
  - Delta Temperature For Minimum Fan Speed
  - Delta Temperature For 100% Fan Speed
  - Cooling Liquid Heat Capacity
- Temperature Control Manual mode—Used to verify the water flow rate after the cold water supply has been connected. When the water flow rate has been validated, use the Auto mode setting.

  In this mode, the MCS unit operates, manually, according to the settings you have assigned to the following parameters:

  - Fan Speed Target
  - Water Valve State

Systems Insight Manager integration

In this section

Systems Insight Manager overview

Use HP Systems Insight Manager to:

- Discover management modules. As part of the discovery process, HP SIM can detect an installed management module. The web interface for the discovered module can be launched from the HP SIM Servers Links tab.
- Receive SNMP traps from the management module. The management module can send event-based traps to HP SIM that include a URL in the trap. This functionality enables administrators to easily launch the web interface of the management module in context. For example, if the management module detects an alarm condition, the management module can send a trap to HP SIM with an attached hyperlink that routes users directly to the web interface for the attached management module.
- Conveniently launch the management module web interface from within HP SIM.
  - Tools menu—You can add a link to the web interface on the HP SIM Tools menu using a tools definition file.
  - Servers Links tab—The web interface can be launched from the HP SIM Servers Links tab.
  - Event-based trap—A URL is included in each trap to link directly from HP SIM to the web interface for the specific device for which the trap was sent.

The management module can be configured to send alert traps to Systems Insight Manager, and other SNMP management applications.

To send event alert traps to Systems Insight Manager:

1. Configure HP SIM to receive traps ("Configuring HP SIM to receive traps" on page 50).
2. Configure the management module to send traps to HP SIM ("Configuring the management module to send traps to HP SIM" on page 51).

Discovering the management module

HP SIM automatically detects management modules as part of the device discovery process. If detected, a hyperlink is included on the HP SIM Links page for the HP Modular Cooling System on which the management module is installed. The management module should be installed and running before attempting discovery through HP SIM.

If a link to the HP Modular Cooling System on which the management module is installed does not appear on the device home page in Systems Insight Manager:

1. Locate the additionalwsdisc.props file in the CONFIG directory in the Systems Insight Manager install directory. By default, Systems Insight Manager is installed in the C:\Program Files\HP\System Insight Manager directory.
2. Create a management module entry in the additionalwsdisc.props file. For more information on editing the additionalwsdisc.props file, see the additionalwsdisc.txt file located in the same directory.

Example: The additionalwsdisc.props file with a management module entry

```
#-------------------------------------------------------

#Additional Web Server Discover Properties

#-------------------------------------------------------

#NOTE: See "AdditionalWsDisc_README.txt" for a description of entries in
this file and how to add or remove additional web server ports for discovery
and identification.

#-------------------------------------------------------

The following are actual web server ports enabled by default.

#To remove them from the discovery process, comment out the line with a '#'
or remove it. You will need to restart the HP SIM service for the changes to
take effect. In addition, you will need to run the Device Identification
task to find any new ports that were defined.

#-------------------------------------------------------

#411=Director Agent,,true,false,,http

#3201=Compaq TaskSmart,,true,false,,https

#8008=Default Home Page,,true,false,,http

#1311=Server Administrator,,true,false,,https

#1234=HP Modular Cooling System,,true,false,,https
```

The last entry allows System Insight Manager to detect management module installations that are running on port 1234 and using HTTPS.

Configuring HP SIM to receive traps

Before HP SIM can receive traps, the correct MIB file (cpqwcrm.mib) must be compiled into HP SIM.

To register the MIB:

1. Copy the .MIB file from the MCS documentation CD MIBs folder to the HP\Systems Insight Manager\mibs folder.
2. From the HP\Systems Insight Manager\mibs folder, run `mcompile cpqwcrm.mib` from the command line to compile the new .MIB file. A new file named cpqwcrm.cfg is created.
3. Register the new .MIB file by entering `mxmib -a cpqwcrm.cfg` from the HP\Systems Insight Manager\mibs command line.
4. Enter `HP\Systems Insight Manager\mibs>mxmib` at the command line, and verify that the new .MIB file is listed.

> **NOTE:** For more information on uploading and registering a MIB in HP SIM, refer to the *HP Systems Insight Manager Technical Reference Guide* located on the HP Management CD.

Configuring the management module to send traps to HP SIM

1. Add the HP SIM server as an SNMP trap recipient on the Trap Receivers tab (on page 35).
2. Configure the management module to send alert notifications to HP SIM.

Security considerations

In this section

Security considerations overview

The management module implements strict security for two important reasons:

- The module manages devices that have the potential to perform operations that are sensitive and destructive.
- The management module has browser accessibility.

To better ensure the security of the management module and the devices it manages, consider the following topics in accordance with your organization's security policies and the environment in which the module will operate.

- Remote access to the management module requires a user account. Logging in requires the use of a user name and password, which should be kept properly secured.
- Each account can be given different access levels, providing different capabilities. Ensure that the appropriate access level is granted to users.
- Browsing to the management module can be done using SSL, which encrypts the data between the browser and management module. The module is supported by a 128-bit encryption level. SSL also provides authentication of the management module by means of its digital certificate. Securely importing this certificate must be done to ensure the identification of the management module.

Frequently asked questions

In this section

Frequently asked questions

Question	Answer
How many user sessions are supported at one time?	Only one user session is supported at a time. Sessions can be terminated if a second session is initiated or if a console session timeout occurs.
How many Admin sessions are supported at one time?	Only one Admin session is supported at a time. Sessions can be terminated if a second session is initiated or if a console session time-out occurs.
Why does my Admin session keep getting disconnected?	If a second Admin session is initiated, the existing session is terminated and the login screen appears.
Why can I not login using my FTP user name and password?	FTP Admin and Users are blocked until the Admin assigns passwords and FTP is enabled in the Management menu of the Remote Access tab.
How do I upgrade my firmware?	For more information, see the Support Pack instructions included with the firmware upgrade.
How do I change the management module IP address?	You can change the management module through the Network menu (on page 33) or through the serial interface. For more information on changing the management module IP address through the serial interface, see the *HP Modular Cooling System User Guide* on the documentation CD included with is kit.

Why do I get an extra line feed sent from Windows® when I access the serial interface connected through a HP 16- and 48-Port Serial Console Server?	You must assign this command to the HP 16- and 48-Port Serial Console Server, where port X is the port where the MCS unit is connected.
	`port x set out If=strip`
	`port x set flow=Xonxof`

Why are FTP admin and user logins not recorded in the FTP.log?	Only FTP file uploads are recorded in the FTP.log.
Can I assign the SSL default port 443 as a non-SSL port?	Yes, you can configure any port, including port 443.
Why is the configuration file, when restored, not appearing in the FTP upload directory?	The configuration file is restored in another directory.
Why are active alarms appearing after I power-cycle my management module?	The alarms are updated every 30 minutes. If you power-cycle the management module in-between this time frame, the alarms are still active and appear. After power-cycling the first time, clear the alarms, wait 30 minutes, and power-cycle again.

Question	Answer
Why are my event.log and alarm.logs not formatted correctly when I download them in .bin mode?	The event.log and alarm.log are not formatted to be downloaded in .bin mode. Use ASCII mode.
Is there a confirmation that my system is being restarted after I select the Restore to Factory Defaults or Restart buttons, or after I restore a configuration?	No, there is no confirmation that the system is being restarted.
Why is the web browser not responding when I enter the management module IP address?	• SSL might be enabled. Enter `https://`*hostname[:port number]* where *hostname* is the IP address of the management module and *port number* is the port you assign for SSL. • You might have assigned a port number other than 80, or changed the port number in the Remote Access tab. Enter `http://`*hostname[:port number]* where *hostname* is the IP address of the management module and *port number* is the port you assigned in the Remote Access tab. For more information, see the "Remote Access tab."

Replaceable parts and maintenance and service information

In this section

Replaceable parts

The heat exchanger units and fan units are replaceable during real-time operation. Other unit parts are also replaceable. For more information on replaceable parts and CSR parts, refer to Technical support.

Acronyms and abbreviations

CSR

Customer Self Repair

DHCP

Dynamic Host Configuration Protocol

DST

daylight savings time

FTP

file transfer protocol

GMT

Greenwich mean time

HTTP

hypertext transfer protocol

HTTPS

hypertext transfer protocol secure sockets

IP

Internet Protocol

MCS

modular cooling system

NTP

network time protocol

SNMP

Simple Network Management Protocol

SSL

Secure Sockets Layer

Index

T

U

W